1 FEDERAL ENERGY REGULATORY COMMISSION

2

- - - - - - - - - - - - - - - - - - x
3 In The Matter Of:
vERSION 5 CRITICAL INFRASTRUCTURE PROTECTION
4 RELIABILITY STANDARDS

5 RM13-5-000

6 - - - - - - - - - - - - - - - - - - x

7 Commission Meeting Room
Federal Energy Regulatory Commission
8 888 First Street, Northwest
Washington, DC
9 April 29, 2014
10:00 a.m.
10

11 BEFORE: MICHAEL BARDEE

12 Appearances

13 Michael Bardee, Chair
Keith O'Neal
14 Daniel Phillips
Harvey Lloyd
15 David DeFalaise
Jonathan First
16 Kevin Ryan
Matthew Vlissides
17

18 * * * *

19

20

21

22

23

24

25

1 (Panel 1)

2 Panel 1

3 10:15 - 11:45 p.m. The Adequacy of the CIP version 5

4 Standards for Protection of BPS Communication Networks

5 Dan Skaar, President and CEO, Midwest Reliability

6 Organization

7 Perry, Director, CIP, Southwest Power Pool Regional
Entity

8 Richard Dewey, Senior Vice President & CIO, NYISO

9 Steven Parker, President, EnergySec

10 Mikhail Falkovich, Manager NERC/CIP Compliance, PSEG;

11 Speaking on behalf of Electric Power Supply Association

12 Tobias Whitney, Manager, CIP Compliance, North America

13 Electric Reliability Corporation (NERC)

14 * * *

15 MR. BARDEE: Good morning,

16 everyone. Thank you being here today.

17 We scheduled this for a nice rainy

18 day so you would have no excuses to skip

19 this event. Nice to see you all here.

20 I am Mike Bardee. I am the

21 Director of the Office of Electric

22 Reliability here FERC.

23 Before we get to the substance of

24 today's agenda, let me go over just a

25 few administrative details.

1 We have a room next door, Room 2,

2 and it is available for coats, jackets

3 and related things, so if you would like

4 to drop those off there.

5 In case of an emergency today,

6 please take the stairs with the

escalator down to the ground floor and exit the building and not use the elevators.

In terms of what you can bring into the room, only water is allowed, no coffee, no food.

We will have the discussion today transcribed. We have a court reporter present taking transcription and that transcription will be posted within a couple days or in a few days at most.

We are also going to be issuing probably tomorrow a notice setting a deadline for people to file comments on today's discussion and topics if they choose to do so.

We have not decided on the deadline yet, but that will be part of the notice that gets issued later this week.

If anyone would like to submit comments, please feel free to do so on the docket number and within the deadline specified in the notice.

At lunch time the Sunshine Cafe is available. There are other locations nearby that you can get to by either walking up First Street either way, there is Union Station and hopefully it will not be raining heavily at lunch time.

I request as to your cell phones and other electronic devices that you may have to please put them into silent mode so we do not have disruptions. Just one other matter administratively.

We laid out a time line in the notice for today's agenda of when the panels will be, depending on how the day goes, and any given panel may run longer or shorter, we will just adjust the schedule as the day goes on as necessary.

Turning now to the substance of our discussion today. As you all know, the

Commission approved Version 5 of the critical infrastructure protection reliability standards back in November of last year, and in doing so, the Commission directed NERC to prepare and submit some changes in a few areas.

We will not be spending much time today on those particular directives, but really, the focal point here today are some other issues that were highlighted in the Commission's order and for which the Commission directed staff to hold this conference here today and I will just describe them very briefly and they were stated in the

16 notice that went out for the conference
17 today.
18 One of the issues was the adequacy
19 of the Version 5 Standards regarding
20 data being transmitted over data
21 networks.
22 The second had to do with whether
23 additional security controls or other
24 measures were needed to protect
25 communication networks including issues

1 about remote system access.
2 The third topic highlighted in the
3 Commission's order for discussion today
4 had to do with how the Version 5 of the
5 CIP Standards relates or compares to the
6 frame works issued by NIST, the one
7 issued earlier, and then the more recent
8 one, the risk management framework.
9 That's a very brief summary of the
10 topics for today.
11 Our first panel is here to address
12 the question of the CIP 5 Standards and
13 data being in transit.
14 Let me turn to the speakers and I
15 will introduce them as we proceed.
16 I will start with Dan Skaar. Dan
17 is the president and CEO of the Midwest
18 Reliability Organization, one of the
19 regional entities within NERC, and so I
20 would ask Dan if you will kick us off

for the day.

MR. SKAAR: Good morning, and thank you for the opportunity to provide comments.

My name is Dan Skaar and I am

President and CEO of Midwest Reliability Organization.

I am not participating in my official capacity today, so my comments do not necessarily reflect the views of the my Board.

The Bulk Power System has become more secure as a result of the CIP Standards.

Industry awareness of security matters has increased significantly over the last few years and state utility commissions and the NARUC are actively promoting security for consumers at the distribution level.

We are all here because we know we have more to do. I have three suggestions for your consideration.

After World War I, the French built the Maginot line to secure its borders from invasion.

They were comforted by this sophisticated costly fixed fortification.

A year after its completion, the

Maginot line was rendered useless in a matter of days bypassed and outflanked in World War II.

We know the rest of the story.

My first observation is we must prevent the CIP Standards from becoming like fixed fortifications destined to be monuments rather than protection.

So how do we proceed?

We must be aware of the cost and confusion created by forever changing the CIP Standards.

The Version 5 standards can serve as the foundation for security provided we - the industry and regulators - are mindful of new technology and ever-changing risks so we "future proof" the standards.

Virtualization illustrates the point. Virtualization has the potential of creating mixed trust environments.

Version 5 does not directly address this situation.

Emerging communication technologies deployed in substations may pose similar

challenges.

Guidance and security frameworks may be necessary to complement standards in order to "future proof" them.

My second observation is cyber security for our industry is about systems.

It is not discrete risk. It is systems risk - a complex system of systems.

Fortunately, Version 5 is more focused on systems than previous versions of the CIP Standards. This is consistent with my long-held view of assessing risk on complex systems.

It should be a "tops-down" exercise starting with the supervisory controls systems, SCADA, focusing on the central nervous system downward to the fingers and toes and recognizing the interdependencies including communications.

In the context of systems risk we should emphasize connections such as ICCP between neighboring systems

regardless of size just as much as connections within an a single system.

After all our mission is to prevent uncontrolled cascading events.

We are only as strong as our weakest link.

For MRO and two other regions this is also an international endeavor because we share the interconnection with Canada so security interests must include our northern neighbors.

Let me describe what happens when we do not use a tops-down approach to system risk.

Recently, I participated in a Version 5 transition study. Thirty highly skilled people spent an hour discussing compliance around a device located inside a secured physical perimeter that only could be reprogrammed by disassembly, reflashing the EPROMs and then reassembly.

Reprogramming this device required physical access, specialized knowledge, and specialized equipment.

There was a lot of anxiety. This was not a systems approach to risk, but rather a fingers and toes compliance mind set.

Is it programmable? Yes. Is it a high-security risk? No.

In this situation, the probability for intentional, harmful manipulation is low. It is a discrete risk having little potential to contribute to an

uncontrolled cascading event.

On the other hand an RTU communicating through routable protocol from a non-BPS asset may pose risk. An individual may have easier access to the RTU at the substation because it is likely not governed by the CIP Standards and may create risk to the control system's front end.

This clearly poses more risk than my first example, but I want to be very clear.

I am not implying that non-BPS assets or assets not designated as critical are not secure.

Responsible entities have obligations to consumers to maintain secure systems.

But I don't know what I don't know and the fact that I don't know the nature of communications with key systems like supervisory control of the bulk power system raises concern.

It may not be a risk, but it's a known / unknown which should be addressed in some manner.

Simply put, we must not confuse compliance with security risk causing industry to invest more in low probability matters at the expense of

16 higher risk items.

17 We need to find ways to optimize

18 investments by using tops down

19 approaches to system risk and if we do

20 not address important communication

21 interdependencies through the CIP

22 Standards we should at the very least

23 address them through guidance and

24 security frameworks.

25 My third observation relates to

1 enforcement. Cyber security is complex

2 requiring diverse perspectives.

3 It is not a perfunctory legal

4 process. It's a technical problem

5 solving activity requiring frank

6 engagement and we need to promote

7 problem-solving which allows entities to

8 fix deficiencies without an enforcement

9 proceeding.

10 This is a rational regulatory

11 approach and we can still have

12 transparency, and of course, we always

13 have the enforcement tool for serious

14 matters.

15 We need to adopt a fix it first

16 approach and I believe the Reliability

17 Assurance Initiative can deliver on

18 this.

19 In summary, Version 5 can be

enduring and be designed in a way that is valued by the industry. It should be akin to a UL listing. We can improve the value of the CIP Standards by doing the following:

First, consider methods to

future-proof the standards so that they can adapt to new technologies and emerging threats.

Second, emphasize tops-down approaches in assessing security risks to recognize interdependencies including communications.

Third, adopt a fix it first regulatory posture. Thank you.

MR. BARDEE: Thank you, Mr. Skaar. Next, is Kevin Perry who is the Director of Critical Infrastructure Protection for the Southwest Power Pool Regional Entity.

Mr. Perry.

MR. PERRY: Good morning. My name is Kevin Perry. I am the Director of Critical Infrastructure Protection at the Southwest Power Pool Regional Entity.

Thank you for inviting me to speak on the adequacy of the CIP Version 5 Standards for the Protection of Bulk Power System Communication Networks.

The CIA Triad, in other words,

confidentiality, integrity and availability, is one of the core principles of information security.

In the electricity sector, I believe integrity and availability are critical. Without timely, accurate data, the ability to maintain situational awareness and to control the Bulk Power System is severely hampered placing the reliability of the Bulk Power System in jeopardy.

Confidentiality, while important, is not as critical.

While not necessarily easy to do it is possible to intercept and manipulate data via a man-in-the-middle attack.

Data can be changed or replayed to make the operator assume incorrect operating conditions and to respond improperly.

DNP3, a protocol commonly used to communicate data between the control center and the field assets is vulnerable to buffer overflow and other injection attacks irrespective of

whether the data is transmitted via a

routable protocol.

Data can also be manipulated or control command sequences inserted to cause the unintended operation of field equipment.

The ability to intercept and manipulate data has been demonstrated in a variety of classified and unclassified settings and the data can be intercepted to obtain information about current operating conditions that could be valuable in crafting and carrying out a successful attack against the Bulk Power System.

These attacks are simplified by the fact that the data is often transmitted in clear text and without end-point authentication or integrity verification making the data manipulation easy to accomplish.

Today the CIP Version 3 Standards require only that the communication network systems serving as Electronic Security Perimeter Access Points and any

communication network devices and infrastructure residing within the ESP be protected under the CIP Standards.

These protections consist of a combination of basic logical and

physical controls including the requirement that these devices be subjected to physical and electronic access controls and managed per a variety of administrative and technical controls.

The standard explicitly excludes any communication infrastructure outside of the ESP including communications between ESPs.

The FERC-approved definition of cyber asset as applied in the CIP Version 3 Standards includes data which was understood to mean both data in motion and data at rest.

To protect data in motion the registered entity was expected to physically protect the cabling over which the data were transmitted within the ESP.

The standard does not require encryption or other controls to protect the data communicated outside of the ESP.

It quickly became apparent that physically protecting the data in motion was problematic given the pre-existing characteristics of the critical asset and the design of the communication networks.

FERC approved an interpretation of CIP 6 requirement R1.1, on July 15, 2010, allowing for alternative physical or logical protection controls in lieu of a six-wall boundary.

Essentially, this interpretation recognized and addressed the problems with protecting data in motion when the data and its transmission media could not be contained within a six wall boundary.

On March 21, 2013, FERC remanded an interpretation of the same requirement that sought to exclude data cabling and thus data in motion from the CIP

Standards when the Electronic Security Perimeter was not entirely contained within a single ESP.

While the application of CIP 6 requirement R1.1, as interpreted, serves to protect the data within the ESP it still does not protect data in motion between the ESPs or between the ESP and any field cyber assets not subject to the CIP standards.

At audit I have seen a variety of protections for data within a control center ESP. Those controls include the physical protection of the network

communication devices and data cabling within the control center facility and the control of electronic access at the ESP network perimeter.

While not required by the CIP standards, I have also seen, albeit not consistently, the use of encrypted VPN tunnels between the primary and backup control center ESPs.

However, I have also seen where the registered entity has implemented or

continued the use of a non-routable protocol between the control center and a field asset for the express purpose of keeping the field asset out of scope of the CIP standards.

The use of a routable protocol to communicate beyond the confines of an ESP is a determinant for identifying critical cyber assets and registered entities are legitimately leveraging that determinant to minimize the number of critical cyber assets they have in the program.

Unfortunately, I have also seen registered entities attempt to argue that the use of multiprotocol label switching, or MPLS, for their wide area networking is not communication using a routable protocol because data is

directed from one network node to the next based on short path labels rather than long network addresses avoiding complex lookups in a routing table.

Similarly, I have seen entities argue that a routable protocol was not

in use because the data was going, in part, through a Layer 2 switch or that a relay was not communicating outside the ESP with a routable protocol because it was serially connected to an RTU that was in turn communicating with a routable protocol.

In those instances, the registered entity was advised of non-compliance with the CIP standards.

The CIP Version 5 standards as currently approved have made some substantive changes to address the security gaps present in today's CIP Standards.

There remains significant gaps that can in many cases be readily addressed without excessive expenditure of resources and the CIP Version 5 Standards took a step backwards with respect to communication networks and data.

As FERC noted in Order 791, the

definition of cyber asset was modified to remove communication networks from

the definition and to limit data to that residing within the device also known as data at rest.

I see two gaps with respect to communication networks.

First of all, routable data communicated between ESPs should be encrypted.

This presumes an ESP or electronic access control of some sort at assets containing low impact BES Cyber Systems.

For data communication between ESPs, the encryption can be readily established by defining an encrypted VPN tunnel in the firewall or router at each end of the communication path.

If an ESP has been extended across multiple geographically dispersed assets where end-to-end physical control of the communication network cannot be maintained high-speed encryptors are commercially available that will encrypt the data as it travels between the physical locations.

The data encryptors are not viewed

as ESP access points and there is no expectation of attempting to impose electronic access control beyond the connection negotiation between the two devices.

Registered entities should also consider encrypting non-routable data traffic between the control center and the field asset, in other words, the RTUs and the relays in the generation plants and transmission substations.

There are in-line or bump in the wire solutions available to address this need.

Encryption should be avoided however if the data latency introduced by the encryption process could cause the intended operation to fail.

An example of data latency risk is found in protective relaying schemes where millisecond timing is needed to protect the equipment from damage.

Ideally, the data in motion should also be cryptographically hashed in order to detect modification and

date/time stamped to detect a replay attack.

Hashing and date/time stamping are not widely used today and are not something that can be easily introduced,

but they are far superior to protecting the integrity of the data than can be accomplished with encryption alone.

Secondly, some sort of protections should be extended to the communication network infrastructure outside the ESP where the registered entity has administrative management control over the hardware.

The NERC Reliability Standard COM1-1.1 and I understand COM2 has taken some information out and IRO 2 is being worked on to reinsert it requires each reliability coordinator, transmission operator, and balancing authority to provide adequate and reliable telecommunications facilities for the exchange of interconnection and operating information.

The standard requires that

telecommunications facilities to be redundant and diversely routed where applicable.

The purpose is to provide high availability of the critical communication networks both local and wide area.

The CIP Version 5 Standards should require the registered entity to protect

the cyber assets used to provision these networks to the extent the registered entity has administrative control over the assets.

No one expects the registered entity to impose the CIP Standards on a commercial carrier such as AT&T, but the registered entity can certainly apply some aspect of the CIP Version 5 Standards to the equipment it manages.

I suggest that modifications be made to the CIP Version 5 Standards to address both of these gaps that at a minimum restrict physical and electronic access.

In summary, while the CIP Version 5

Standards have made substantive changes that will close a number of security gaps present in the Version 3 Standards, two significant communication network gaps remain that should be addressed.

The integrity of the data relied upon for Bulk Power System reliability needs to be protected during communication by encryption at a minimum and where possible through the application of cryptographic hashing and date/time stamping.

The critical communication network cyber assets outside of the electronic

security perimeter, but under the management control of the registered entity need to be protected through the application of an appropriate set of security controls.

Thank you for the opportunity to provide opening remarks for this technical conference and I look forward to the discussion to follow.

MR. BARDEE: Thank you, Mr. Perry. Next, we have Richard Dewey and he is

the senior vice president and chief information officer for the New York ISO.

MR. DEWEY: Thank you, and thank you for the opportunity to present at this panel.

My name is Rich Dewey and I am senior vice president of the New York ISO and the NYISO is responsible for operating New York's high-voltage transmission network, administering and monitoring the wholesale electricity markets and planning for the state's energy future.

The information technology group that I oversee is responsible for delivering products and services to evolve the wholesale electricity

markets; development, support, and maintenance of all NYISO software and systems, strategy development, technical design, and maintenance of the NYISO's computing infrastructure.

Additionally maintaining the NYISO's physical facilities and

enterprise security both cyber and physical.

I would like to thank the Commission and FERC staff for the opportunity to participate in this technical conference to discuss the critical infrastructure protection topics identified by the Commission in Order 791, and more specifically, to participate in the panel on and provide these comments regarding the adequacy of the approved CIP Version 5 Standards for protecting data being transmitted over Bulk Power System communication networks.

The New York ISO working with its stakeholders, peer ISOs/RTOs, and the broader electricity industry strives to be a leader in addressing cyber security issues related to the protection of critical infrastructure.

To that end the NYISO regularly participates in standards development

processes, works with industry groups, and engages in regional, national, and

international planning initiatives addressing future technology and security integration.

The NYISO is currently supporting the standard drafting team addressing NERC Project 2014-02 CIP Version 5 revisions which formed to address the points raised by the Commission in Order 791.

Keeping the lights on is always the primary focus for the NYISO. Cyber security is critical to that effort.

The NYISO recognizes the importance of robust CIP standards, and notes that standards such as CIP-005 have protected electric grid operations from cyber attacks such as the Shamoon by using computer network segmentation to restrict access to the critical infrastructure.

But would-be attackers quickly adapt and so must industry by continuously evolving our security posture in response to rapidly changing risks, threats, and technological

advances.

In this way cyber security standards must enable rather than hinder continuous improvement.

The NYISO supports the trend in cyber security rulemaking toward standards that are not needlessly prescriptive, but rather where appropriate give entities the latitude to identify and assess enterprise-specific risks and develop appropriate controls to mitigate them.

The NIST framework is an excellent example of such an approach. Given the substantial volume of sensitive data the NYISO must continuously exchange with its market participants, neighboring control areas and other interested parties and securing our communication networks is particularly essential.

With respect to the NERC CIP Version 5 revisions now underway at NERC, the NYISO recognizes that concepts such as the use of strong encryption and network access controls are elements

that any user or operator of a communications network must strongly consider.

At the same time we recognize the

inherent difficulty of drafting cyber security standards that reflect the varying needs of industry members with different network topologies.

To that end, the NYISO urges NERC and the Commission to employ a risk-based methodology for any new or revised CIP Standards related to communication networks in order to encourage and leverage well-tailored and cost-effective controls like those that will be described further in these comments.

Communications network protection will necessarily involve a combination of architectures, technologies, and embedded solutions such as monitoring.

Entities should be empowered by any new or revised standards to find the combination of these controls that are appropriate to the levels and types of

risk they identify.

The telecommunications industry, a distinct critical infrastructure in its own right, is a driving force for enabling innovation by electric utilities.

With the advent of new telemetering sources like phasor measurement units or PMUs, coupled with the need to monitor

the dynamic characteristics that other technologies like battery storage, increased renewable energy, microgrids and distributed generation are adding to the grid, the need for real-time or near real-time data has never been greater.

Advancements in communications networking provide means to collect and disseminate data with greater ease and at ever increasing rates as the electric industry becomes increasingly reliant on such data exchange securing communication networks grows ever more critical.

I would like to make the Commission aware of two initiatives reflecting how

the electric industry is proactively addressing the need for secure communication networks.

First, the NYISO is supporting an effort by our industry and its trade groups to implement a Department of Energy supported effort to identify appropriate cyber security procurement language for control systems.

Despite our industry's heavy reliance on networking telecommunications remains a complementary yet separate form of

infrastructure.

This means that at least for the foreseeable future we are heavily reliant on external service providers to assist us in developing and securing our communication networks.

By collaborating to identify and document best practices for cyber security technology including for networks protection industry is developing a common language to communicate to and obtain from its

vendors the security architecture needed to accomplish its core purposes.

Second, in the spring of 2013 the New York ISO and other reliability coordinators in the eastern interconnection cataloged a number of operations data transfer mechanisms that occur through a variety of mediums.

We identified an opportunity to provide additional capabilities particularly as PMU data is incorporated into situational awareness, and a shared desire to investigate mechanisms to obtain consistency and efficiencies in securely managing these data exchanges.

That effort culminated in the formation of the Eastern Interconnect Data Sharing Network, Inc., EIDSN, a

non-profit corporation formed in January 2014.

The EIDSN is positioned to build and coordinate the reliable and secure exchange of critical infrastructure information amongst its members.

Its design team is currently

identifying the security architectures necessary to safely share critical operational information.

The EIDSN will translate those requirements into a request for information and request for proposal for bidders to propose solutions to provide these essential services for the organization and the industry.

It will rely on the cyber security procurement language for control systems discussed previously and our collective experience with Smart Grid projects to help ensure security is embedded into the life cycle of EIDSN services and products.

Initiatives like the cyber security procurement language for control systems and EIDSN demonstrate the commitment of the NYISO and our industry to promoting and enhancing secure networking capabilities that reflect the evolving

needs and demands.

Just as importantly, these are real world examples of industry's success in

identifying risks and relying on its expertise to develop means to mitigate that risk.

Any additional CIP Version 5 Standard language should reflect that approach.

As cyber security matures tools to share sector-specific information quickly and securely grow increasingly important.

One such tool is the reliability coordinator information sharing portal, RCIS, which enables the exchange of incident and threat-based information along with reliability data.

Electric industry reliability coordinators and balancing authorities are uniquely situated at the crossroads of this information exchange possessing strong system visibility and operational knowledge to interpret this data, maintain grid reliability and restore operations after an event.

Secure communication networks are vital to leveraging these capabilities.

More broadly, industry continues to work with public and private organizations to improve sharing of cyber and physical security threat information and assessments to support its core business practices and in response to Executive Order 13636 and Presidential Policy Directive 21.

The Electric Sector Information Sharing Analysis Center ES-ISAC, working with government partners is aiding this effort with its Industrial Control Systems-Cyber Emergency Response Team or ICS-CERT, coordination activities.

The Department of Energy cyber risk information sharing program and cyber fed model also offer promise for developing enhanced and cost-effective tools to increase information sharing in gain situational awareness.

NERC's GridEx II preparedness exercise in November 2013 also demonstrated industry improvements in sharing security-related information.

NYISO fully participated in NERC's

GridEx II exercise with many other organizations, agencies, and entities, communications and information sharing along with regional coordination led to

a successful exercise.

In conclusion, new technologies introduced into the electric grid provide both promise and challenge.

The ability to collect and disseminate new more detailed metering will drive more advanced applications and greater capabilities to address the challenges of incorporating renewable sources of energy into the grid.

Enhanced capabilities for management and monitoring of battery storage, flywheel, microgrid and distributed generation technologies will allow these new grid elements to meet the full potential of delivering resilient and reliable energy for consumers.

Better identification and sharing of situational awareness and threat-based information between and

among industry and government will enhance critical infrastructure reliability.

Communications networking is critical to addressing all these needs.

Appropriate risk-driven security measures must and will be applied as we grow and evolve the communications

networks used in our industry.

The New York ISO looks forward to addressing this challenge with industry and government partners. Thank you.

MR. BARDEE: Thank you, Mr. Dewey. Next, we have Steven Parker. He is the president of Energy Sector Security Consortium otherwise known as the EnergySec.

Mr. Parker.

MR. PARKER: Good morning. My name is Steven Parker, and I am President of Energy Sector Security Consortium, commonly known as EnergySec.

I would like to thank the Commission for the opportunity to participate in this important panel

discussion addressing the security of communications in the Bulk Power System.

In my opening statement I will discuss this issue as it relates to the NERC CIP standards.

Though not entirely ignored communications are only tangentially addressed in the CIP Standards.

The standards themselves are centered on the protection of those cyber assets deemed to have importance in the operation of the bulk power system, but largely ignore the function

of communication itself.

First, let me point out some notable exceptions.

The requirement for electronic security perimeters which I will refer to as ESPs, results in some restrictions on communications to and from protected cyber assets.

Likewise, the requirement to limit ports and services are both through such perimeters as well as on cyber assets themselves provides another

communication related control.

Communication devices themselves such as switches and routers are often in scope for the CIP Standards, and finally, there are requirements related to remote interactive access.

Despite these examples, significant gaps exist in Version 5 of the standards with respect to communications.

I will briefly touch on three of these areas and hope to expand on these during the balance of the panel discussion.

First, with respect to ESPs and required port restrictions.

The standards allow any and all communication deemed necessary for

operations by an entity even if such communications utilize insecure protocols.

There are no requirements related to the security of the communications themselves.

Second, non-routable communications are entirely out of scope.

In Version 5 all requirements related to ESPs involve only routable communications.

As written the standard and its associated formal definitions can be reasonably be construed to allow any form of non-routable communication to and or from any in-scope cyber asset and any other asset with no protections whatsoever.

This is a significant gap.

Third, communications occurring outside of an ESP are also out of scope. This is significant since most wide area communications occur outside the context of an ESP.

For example, the inter-control center communications protocol, ICCP, is used to exchange operational data between control centers.

Although the servers involved in the process are nearly universally

considered to be in-scope for protection the wide area communications through which the data is exchanged, is

universally out of scope.

I don't believe these gaps to be intentional, rather they are a natural byproduct of requirements which center on cyber assets alone.

Although the focus on cyber assets was a proper first step in early versions of the CIP standards, I believe the time has come to address communications as a function.

To be clear I am not suggesting that specific prescriptive controls are missing from the standards and should be developed.

Rather, I assert that the standards lack defined security objectives for communication functions and that such objectives should be defined and addressed in future versions of the CIP Standards.

Let me explain this further by mentioning two distinct but related topics.

First, in the guidance section of CIP 5 of Version 5, the drafting team

explained that specific requirements for serial communications were excluded since no universally applicable requirements could be identified.

Second, in paragraph 108 of Order 791, the Commission stated that NERC might address the lack of specific requirements for low-impact assets by "developing objective criteria against which the controls adopted by responsible entities can be compared and measured in order to evaluate their adequacy."

We see two concepts here.

First, prescriptive controls can be difficult to construct.

Second, an alternative to prescriptive controls might be to articulate objectives and associated criteria for evaluating whether those objectives have been met.

Such an approach allows entities the flexibility to be innovative in meeting security objectives.

Communications is an area where

such an approach would be appropriate if not necessary.

Communication technologies used in

the Bulk Power System are numerous and diverse.

There is no set of prescriptive controls that would be both appropriate and sufficient for all such communications.

However, it is likely that a set of security objectives for the protection of such communications could be developed and indeed it should be.

To summarize, there are significant gaps related to communications in Version 5 of the CIP Standards.

These gaps should be addressed in future versions, but require a different approach than that currently used.

I look forward to exploring this further in the remainder of this panel discussion.

Thank you.

MR. BARDEE: Thank you, Mr. Parker. Next, we have Mikhail Falkovich and he

is the manager of NERC and the CIP compliance at PSE&G and he is speaking here today on behalf of the Electric Power Supply Association, EPSA.

MR. FALKOVICH: Good morning, and thank you for the opportunity to participate in this important forum.

My name is Mikhail Falkovich and I

am the manager of NERC CIP compliance for PSE&G representing the Electric Power Supply Association.

My comments are focused on the vulnerabilities that the BPS communication networks may be facing and how effectively they are being protected against these risks by the currently enforced CIP reliability standards.

Today, I will discuss the concept of relevant operational data flows and how it fits within the framework of the CIP Standards.

Though some gaps do exist in the currently approved CIP Standards EPSA believes that these gaps will be effectively closed by additional

standard language that the CIP provisions drafting team is currently developing.

In other instances perceived gaps will be best addressed outside of the CIP Standards scope due to the potential BPS reliability risks associated with compulsory encryption based mandatory standards.

There is also a need for flexibility within standard requirements so that the industry can meet its

13 compliance obligations without
14 significantly impacting the reliability
15 of the BPS.
16 It is important to note that the
17 industry has had in its place enterprise
18 level security programs prior to the
19 enforcement of CIP Standards.
20 These programs still apply BES
21 practice risk based security controls on
22 both enterprise and real time systems.
23 The standards require specific
24 artifacts to be created and objectives
25 to be met while at the same providing

1 entities with a flexibility to design
2 their own processes and architectures.
3 CIP Version 5 data security
4 provisions are mandated through
5 requirements dealing with information
6 protection in both physical and
7 electronic security perimeters.
8 In cases where the data objects
9 themselves are not easy to encrypt such
10 as documents or where there is
11 interactive access established to manage
12 a protected system, a VPN tunnel is
13 established to secure connectivity
14 either on a permanent or a per
15 connection basis.
16 Appropriately the CIP requirements
17 for encrypting interactive remote access

clearly identifies that entities must utilize encryption that terminates at the intermediate system.

Let's talk about security options for both LAN and WAN operational data flows in some more detail.

Given control center processes a significant amount of realtime data

between the nodes of its energy management system.

These data flows and the LANs that support them are critical to the operation of such control centers.

On CIP Version 5 the definition of a cyber asset no longer contains the term communications networks and thus creating uncertainty within the industry with the required protections from cabling and non-programmable network components.

To provide additional clarity as to how such communications networks are protected, the revisions drafting team is working on the language that will define the scope of protections required for cabling, transceivers, and other non-programmable devices.

This language provides flexibility to how a given entity is able to secure

its communications network environment either through physical security measures or through the applications of logical security controls.

Additionally without specifically using the term "communication network" the approved CIP Version 5 requirements for BES fiber system information protections still apply to all data but is identified by the registered entities as BES cyber system information.

The flexibility of security control solutions for registered entities is essential to the successful operation of the BPS.

The typical corporate systems utilizing the TCPIP suite of applications are inherently able to support delay within the network.

Realtime systems on the other hand often have operational requirements where data must be processed in a certain amount of time and in less time of delays.

Thus even in a LAN environment the introduction of latency can cause undesired effects within realtime applications.

Depending on the design of the real

time system the communication between those of a given ENS may be configured as UDP broadcast which are very difficult to encrypt within the network.

In these instances the flexibility to use alternate physical security controls is extremely important as encryption may add to the undesired effects to the operation of the BPS.

On the other hand, data traversing wide area networks is extremely difficult to secure via physical means and that is the issue of communications integrity becomes more important in those cases where sensitive data is sent via WAN networks.

The DHS catalogue of control systems security provides guidance to entities as to how best to achieve communication integrity.

The DHS catalogue cautions entities that the application of cryptographic mechanisms within control system environments will introduce latency and must not degrade the operation

performance of the systems.

Additionally, the guidance discusses the potential of denial

service conditions in cases of cryptographic failure and cautions that the use of cryptography should be determined after careful consideration.

This recommendation applies that with the use of cryptography, there is a potential for an adverse impact on the BPS and it should be used on a case by case basis.

The SECRA phase initiative is a good example of a real time system that very sensitive to latency. Even without encryption entities are challenged to deliver the data to its destination with very tight latency requirements.

Mandatory encryption of this traffic would require encrypting the data multiple times along the path and would only add to existing latency concerns.

The final attribute of WAN networks that deserves attention is that no

single entity would have control over both ends of an intercompany communications link.

With diverse technologies often in different ends of a security tunnel both entities must agree upon a common method of encryption.

Due to the nature of such variable cryptographic design for amateurs, and the fact that such links are implemented and operated by multiple entities, the encryptions of such communication networks is not an ideal fit for a set of mandatory standards.

For such WAN operational data flows physical protection requirements would be difficult to enforce and potential encryption requirements would increase the latency of the connections as well as the troubleshooting time in case of networker errors.

Additionally, the LAN links in these examples are either private or dedicated networks which have a more secure posture than the public Internet

connections.

The limited benefits of the extra security measures may not in this case outweigh the potential risk to the operation of reliability of the BPS.

With regard to encryption another important consideration is that the architecture of these systems becomes complex.

The more complexity the more opportunities for errors and the longer it takes to troubleshoot them.

In sum, we support the need for further clarification on the required security of communication networks and believe that the changes being developed by the revision's drafting team are beneficial to the reliability of the BPS and will effectively close perceived gaps.

Within the current draft of the provision language there are clearly defined requirements which allow flexibility meeting the desired security objectives.

While additional security measures can be implemented in a stack manner the technical complexity and potential design complications of cryptography may outweigh the security benefits and are therefore not appropriate for mandatory standards.

The flexibility allowed by the proposed requirements for communication networks is essential in maintaining and improving of the BPS.

Thank you on behalf of EPSA and PSE&G for the opportunity to share our perspective on these complex but vital issues that directly affect our nations electric fuel liability.

MR. BARDEE: Thank you, Mr. Falkovich. Our final speaker on this panel this morning is Tobias Whitney manager of CIO Compliance at NERC.

Mr. Whitney.

MR. WHITNEY: Good morning, and thank you. I am Tobias Whitney, manager of CIP Compliance at NERC.

First, I would like to thank the

Commission for the opportunity to be a part of this important conference.

As the manager of CIP Compliance for NERC, I recognize the need for further exploration and assessment of cyber security issues that impact our sector.

NERC's CIP Version 3 Standards have been in place since March 2010 and the Version 5 standards represent the significant improvement and change over the current Version 3 standards as they adopt new cyber security controls and extend the scope of the systems that the standards protect.

Given the significance of the change, NERC identified the need to collaborate with regional entities and responsible entities to understand how to best implement the Version 5 in a manner that is timely, effective and

22 efficient.

23 To more effectively engage industry

24 NERC established a transition program

25 with the following goals:

1 Goal one is to improve the

2 industry's understanding of the

3 technical security challenges that need

4 to be addressed in order to comply with

5 the Version 5.

6 Goal two is to provide the industry

7 a clear path with the approach the

8 transition from Version 3 to Version 5

9 that includes expectations for

10 compliance and enforcement.

11 Goal three is to understand the

12 effort and required resources needed to

13 manage the transition.

14 In order to achieve the goals, NERC

15 has implemented several program

16 elements.

17 Periodic guidance documents will be

18 developed to keep the industry informed

19 throughout the transition period.

20 The reliability assurance

21 initiative will have alignment with the

22 CIP standards drafting team for Order

23 791.

24 NERC will continue to engage

25 industry through various communication

outreach and training outlets.

Our most significant transition program element to date has been the implementation study.

The implementation study has centered on a representative sample of six volunteer responsible entities that agreed to transition to compliance with Version 5 in an accelerated timeframe.

Study participants were selected based on their history of successful Version 3 compliance, demonstrated effective internal controls and their willingness to commit required resources to their transition.

The implementation study began on October 1, 2013 and will end on June 30 of this year, although certain aspects of the study will continue through April 1, 2016.

During this period the study participants focused their attention on technical solutions and processes in order to provide examples of methods that they can use to address the new

standards.

It is our belief that it's better

to address the challenges no as opposed to after the effective date of Version 5.

Throughout the study participants collaborated with NERC and the regional entities to develop technical and compliance solutions and these solutions are being shared publicly on NERC's website and through other outreach mechanisms.

In terms of communication and security challenges the implementation study is enabling the ERO to work closely with industry to address many of the topics associated with this panel.

For instance, substation BES cyber assets.

Version 5 introduced many communication network components such as SCADA to RTU communications connectivity to relays and other intelligent and electronic devices that reside inside of substations.

Many of these systems and networks were not covered in Version 3 because non-routable connections were not clearly in-scope.

Version 5 requires both routable or IP based connections in addition to serial and non-routable connectivity.

Programmable versus non-programmable, the study participants are helping to draft guidance to help industry understand how to identify networks and systems that will be brought in scope of the CIP standards.

The question of what constitutes a programmable device impacts both the BES cyber asset and the networks that protect them.

As I mentioned, the NERC and the study participants will be working closely to develop additional clarifications along these lines.

Virtual servers and virtual local area networks, these are terms that are not explicitly covered in the standard, however the industry's use of such

dynamic technologies are increasing so as a result we will be providing guidance to define how these systems will be made compliant with the Version 5 Standards.

To close, the CIP standards provide the foundation to address today's dynamic cyber security challenges.

As discussed, NERC is already working on communication security and has been doing so through various

mechanisms.

Through the combination of standards, guidelines, alerts and other NERC compliance and enforcement methods we are confident that we can effectively meet the demands of industry to safeguard the bulk power system.

Thank you.

MR. BARDEE: Thank you, Mr. Whitney, and thanks to all of our witnesses for the remarks that have been made so far.

Let me start with a couple of questions and then I will turn to my

colleagues for their questions.

Mr. Perry, you advocated that we should require encryption for data communicated between EPSs, but you recognize also that it could bring up issues for devices that involve latency problems, a similar problem cited by Mr. Falkovich.

Can you give me a better sense of the applicability, where you think it could be useful without tripping or triggering the kind of concerns about latency?

MR. PERRY: RT scan rates between the control center and the substantiation, or generating plant, are

typically in the two-to-four second intervals, so in many cases the latency there is not going to be a problem by introducing encryption especially if the entity is already using a wide area network in a routable protocol to do the communication as opposed to a four wire twisted pair of point to point serial connection.

Certainly between control centers where you're doing data replication between the primary and backup sites you may be operating consoles in one location and the operating servers in the alternate location.

Again, you are looking at interactive, a three to five second type of response rates data latency there that is not going to be a problem.

You get into a transfer trip scheme or a pilot relaying scheme out of the substantiation using communication between two relays at distant sites that has got a much tighter millisecond level operating expectation and their encryption is probably not appropriate because the latency could result in failure to operate in a timely manner to avoid the destruction or damage to the

equipment.

The same thing was brought up with phasor measurement units, very very high speed data transfer there and very likely that the use of encryption may

interfere with the scan rates of the PMUs which would have a less than a desirable impact on what the whole purpose of the PNU is for.

Those are some examples where I think encryption could be used and where encryption probably should not be used.

MR. BARDEE: Mr. Falkovich, or if the other witnesses have thoughts on places where it might actually be appropriate to either require encryption, or to say that you should use encryption or some alternative to it in this context recognizing your remarks earlier that there are times and perhaps many times or even all in your view where it would not be appropriate to do so.

MR. FALKOVICH: I concur with Mr. Perry's view with regard to the latencies in let us say data replication between data control systems.

There are instances where I feel that encryption actually has a very strong presence within the industry and

I will give an example.

Typically, let's say the communications between the control centers and RTUs are sent over private or leased lines, and in some cases, if the amount of data you need to send is very very large that can get expensive, if you need to get a much larger pipe.

Entities often have available to them corporate level, I will say, enterprise networks that you can pass traffic across at a much cheaper rate.

If latency is not an issue and you want to enjoy the cost savings depending on the architectural environment it makes sense to send it over a less secured network, if you will, and then encryption is absolutely mandatory because then you are sending it across that way.

That being said, I would say that flexibility is still an option, and if I want to choose to send that traffic over a private or a leased line where the protection options are much stronger,

the posture is much stronger and they should be able to make that

determination, but I have seen cases where sending over a less secured medium encryption does make sense.

MR. PARKER: Another example I think that we could cite is with respect to storage and the replication of storage.

A lot of these applications do not have local mobile storage or we've got high availability schemes in place where we replicate data between sites or applications through a storage area network where latency could be a big problem in terms of the performance of those applications and that might be appropriate to use encryption as opposed to some other security or a secured scheme for securing the network itself either through some of the schemes that Mikhail talked about or certainly a private network for some sort.

MR. BARDEE: Mr. Dewey, on a separate topic you mentioned in your

remarks an effort that DOE has underway regarding what I would call supply chain protection guidance, and if I understand this correctly, that document actually just came out.

To my understanding the CIP Version

5 requirements do not have much to say about supply chain issues.

Do you think it is reasonable for us to consider expanding the requirements regarding supply chain issues?

MR. DEWEY: Each entity needs to do a risk assessment and an analysis of their suppliers.

I don't know when you start talking about the span and the scope of different types of services that an entity might need to contract for to meet their needs.

It would be challenging to come up with a one size fits all approach.

That would be easily and readily applicable to the myriad of different services that a telecom or other

provider could offer and our approach was to look at some of that standard language to make sure that you have the right contractual protections as well as set the expectations with the providers of what level of performance and what level of delivery and protections that we are going to want to see on their side and be able to spell that out in plain language, number one, so that you have the assurances that they are taking

it as seriously in the products that they give you as you would in protecting your own system, but also coming up with some standards and some conventions across the industry to the extent that we can collaborate and work together to put all the providers in the same spot to know what the expectation is in terms of that level of service.

MR. BARDEE: I certainly can understand the need for some flexibility given the diversity of entities and products and technologies.

Mr. Parker in a different context

was suggesting that the way the standards should be modified in going forward was to specify objectives as opposed to particular controls.

Do you think that might be a good approach for thinking about supply chain issues going forward?

MR. PARKER: I think it could. It is consistent with the approach of the frame works which is the subject of a panel later today where you can come up with some constructs that you can steer the providers and the vendors into a framework of a consistency in terms of the products and the protections that

they can build into that and then also the weight of having that standard contract language so you have got those protections and you are speaking the same language across from provider to provider.

MR. FALKOVICH: To follow along the same train of thought. I mentioned the DHS catalogue of control system security and another guidance that they provide

is that they encourage entities to obtain contractual assurances from vendors of necessary security measures and such assurances are not available and the DHS encourages entities to implement the compensating measures or explicitly assume the additional risk.

That is right out of the catalogue and the procurement language document is very good. It is very good guidance to entities to make proper relations with their vendors.

If we look at the objectives versus requirements as long as there is flexibility for the industry to implement options, they are not necessarily outlined there, and maybe assumes some of the responsibility on their own side not necessarily mandated requirements but to reach specific

21 objections that does offer a good
22 alternative.
23 MR. PERRY: There's a basic problem
24 that the industry is facing however.
25 When I got up into working with

1 Energy Management Systems back in 1985,
2 the systems were specialized, isolated
3 completely, not interconnected with
4 anything else and they were easy to
5 protect.
6 Today you have got critical
7 operational technology implemented on
8 commercial off-the-shelf systems running
9 Microsoft Windows, Linux, and a variety
10 of other operating systems and running
11 Oracle, running Microsoft SQL.
12 If you're working with specialized
13 equipment such as your relays out in a
14 substation, you have got a very limited
15 set of suppliers. It's a very
16 specialized environment.
17 You can work with them to develop
18 appropriate security controls with
19 Hanson and Switzer relays, and SEL is
20 doing very good from what I have seen in
21 that and I know that there are some
22 others that are also doing as well.
23 But we all look forward to Black
24 Tuesday every month when Microsoft comes

25 out with some lengthy list of patches.

1 We look forward to the quarterly
2 Oracle releases. We look forward to
3 Java updates on a regular basis and
4 Adobe does it more than on a regular
5 basis, and as long as we continue to
6 have systems that are built and
7 implemented for cost efficiency purposes
8 on those types of platforms, we are
9 never going to get ahead of the cart.
10 I am not advocating that we go back
11 to the mainframe computers and the
12 10-Base2, but we need to be cognizant of
13 the fact that we just cannot sit here
14 and wave our hand and say, "Yes, we are
15 going to have all of these security
16 objectives and work with all of these
17 vendors."
18 Microsoft has got a much bigger
19 customer base than the bulk power system
20 and I do not think the federal
21 government has the leverage.
22 I don't think this industry has the
23 leverage and I almost question whether
24 the industry itself has the incentive
25 when you consider that somewhere between

1 20 and 30 percent of operational

technology systems are still running on Windows XP that is not even supported by Microsoft anymore exempt for a fee and then only for a limited basis.

We have got some very basic hurdles to overcome before we can start really seriously talking about secure procurement.

MR. SKAAR: We have long supported standard boilerplate language in anything related to control systems that the industry adopts.

We think that is critical because the vendors need to be accountable for security as well and it needs to flow down to the vendors.

We see a lot of third-party applications which are good because they are giving operators a lot more visibility and responsiveness on the system, but these third party applications introduce potential vulnerabilities.

We think the boilerplate language

should apply to any application that is going on a control system.

MR. PHILLIPS: I have been listening this morning. It sounds like that most of you are opposed to prescriptives, specific controls, bulk

electric system communication networks.

Should we focus our collective efforts towards developing mandatory controls that protect BES data in motion? If so, what would those controls look like?

MR. PERRY: Let me confirm that I don't like prescriptive controls. Prescription controls tend to be short-lived in terms of their usefulness and they tend to be one size fits all which we know doesn't work.

Having a control objective an outcome-based objective is far more superior and then you have got the ability to leverage current and future technology to achieve that objective.

Given that I think you can define some objectives for data in motion based

on the CIA Triad.

If you want to protect confidentiality of the data, then say so. If you want to protect the integrity of the data, then say so rather than coming out saying, "We will use TLS 2.0 or we will an EAS 256 Key Encryption," then define your objectives, and then let the industry look at their resources, look at what is

available out there and then apply the appropriate technology to achieve that objective.

MR. SKAAR: Here's the question I ask operators which is, "How do you assure trust in your control system communications?"

We have to get to a point where you're secure, you're compliant and then they can describe, "Tell me how you establish trust in your communication."

I don't want to be prescriptive because I think being prescriptive creates vulnerabilities for attacks.

I would much rather have questions

like, "How do you establish trust?" rather than prescriptive standards.

MR. DEWEY: It really has to focus on the risk-based assessment. There are certainly situations, critical power system data, that is transmitting over an insecure public network, I believe, that absolutely should be encrypted every time.

Time dependent, latency impacted data that is going between my two EPSs on a private fiber that I own and control both ends of, I don't think that needs to be encrypted.

You need to look at the criticality

of the data that you are trans-criticizing. You need to look at the accessibility of the medium and you need to do a risk assessment and come up with a variable approach that makes sense for that application, that data, and that situation and the standards need to be able to allow and provide for that.

MR. PHILLIPS: Allow me to

elaborate on that point. How would you see that working with the current high medium low structure that we have in the CIP Version 5 Standards?

MR. DEWEY: It fits in pretty well to be honest with you. When you look at communication in the context of that assessment with some minor adaptations I think that that can fit in pretty nicely.

MR. PARKER: I would concur with a lot of the statements that have been made thus far.

As Mr. Skaar pointed earlier, he brought the point of a systems of systems approach and from a risk perspective analyzing any particular communication path is going to have a varied amount of risk based on the

context in which it operates.

One thing that has not been pointed out that is critically important to mention, and just for context I am former auditor, I worked for the WAC region for a while with a colleague of

Mr. Perry.

Currently the audit and enforcement regime mechanism is pass fail. You either are compliant or you are non-compliant.

As it is even with prescriptive standards we still have quite a bit of angst in the industry during audits where there is professional judgment being used where there are disagreements over what certain things mean even in a very prescriptive environment.

If we move to a more objectives-based approach, which I support, it will be imperative that the enforcement and audit approach is changed and adjusts to account for that.

MR. FALKOVICH: I will also echo everybody's comments and I will reiterate two points that I mentioned previously.

One is the BES cyber system information entities are mandated to secure it, to protect it.

Already you have kind of an

objective where if you deem that data whether it is in motion or not is BES cyber system information and you need to protect it.

There's your mandate of requirement where I would say in this case it is really an objective because that is an open ended statement and the entities are actually already doing that analysis under the Version 5 Standards.

Once again, I will caution on prescriptive controls. If you are going to mandate encryption by default you are making the systems more complex.

You have to be mindful of availability and troubleshooting.

Operational considerations need to come into account.

If I have an encrypted link, there is much more time involved for me to troubleshoot, for the industry to troubleshoot issues with application if you cannot see the data and to put in an extra infrastructure to actually do that decryption and re-encryption it becomes

more difficult and more complex where

complexity just builds upon itself.

Having objectives and flexibility with meeting those objectives really makes a lot of sense to me.

MR. WHITNEY: My thoughts are along those lines. In addition there also needs to be some pretty clear performance objectives of networks from an operational perspective.

We all mentioned the high availability of our environments and there is a level of comfort that I think the industry needs to be at in terms of understanding how they could possibly overlay technologies that may impact the operational or availability aspect of communications, so I think that is a key piece.

MR. PERRY: I do want to bring up one thought keying on Mr. Dewey's comment about risk.

I haven't been a friendly benevolent auditor all my life.

I have actually built energy

management systems and I have administered energy management systems and I have worked in the control center.

Our SCADA EMS systems today are designed to deal with garbage data.

But there is a limit, so any risk basis that you may have with respect to data protection really needs to have as a primary determinant the aggregation of the data, the span of control if you will.

If I have a communication path from my RTO in a substantiation to my control center over a four wire twisted pair, 1200 baud, and somebody gets in the middle of it where maybe it is going over microwave, and somebody gets in the middle of it and messes with the data, we are talking one RTU's worth of data.

Estimators can figure that out really quickly and they can flag it as highly suspect with the opportunity to investigate.

But when you start aggregating large amounts of data, whether it is

Smart Grid technology or an aggregation of RTUs into an intermediate site that then forwards on to the control center, data from a large area, or ICCP to the reliability coordinator, all of the entity's data, 100 percent of it is over that ICCP pipe.

If you intercept and mess with that data, you have a much broader impact that is basically going to overwhelm

your SCADA EMS system to be able to detect and deal with that.

When you talk about objectives for control and you focus on the more risky stuff it is the aggregation of the data, it is the ICCP data, it is the data between control centers.

That's the kind of data that we are really talking about that needs the most protection.

I could really care less about the RTU, to the communications front end, because my robust system will figure that out for me.

MR. PHILLIPS: With those comments,

I would like to open it up to the rest of the panel.

What are your views about the biggest security threats facing the bulk electric system right now and how will those threats and risks change in the future as the Smart Group become more likely deployed?

MR. SKAAR: I think in the context of cyber risk you are talking about right, and not physical risk, the risk I see is like the STUC Mut example, it is where something is introduced to a control system, the supervisory control

that damages equipment and then blinds the operator from what is really happening which creates a cascading event.

We need to be cognizant of what we are all about. It is preventing cascading events. It is system risk and not discreet risk.

While you need to keep that mind, that is the high-risk stuff, so it is supervisory control and having the

introduction of a vulnerability like STUC MUT or some other type of variant.

MR. PERRY: I agree with Mr. Skaar. The zero days and the variety of ways to get into the system are certainly risky, but I will tell you the same thing I told the SVP RE Board of Trustees meeting yesterday and that is we don't know what is hitting us. We are not very good at this job yet.

The maturity of the cyber security model as deployed in the electricity sector is still very weak.

We have got very basic controls where we are still focusing on compliance. We are avoiding the risk non-compliance rather than focusing on security.

We still have nonsense in our

standards that says that we can review our cyber security logs every 90 days.

I have actually seen an entity that is looking at their firewall logs every 90 days with the Mk-1 Eyeball, and I ask them, "How is that working out for you?"

They answer,"We haven't found anything." Big surprise!

Our biggest risk is that we don't know what we are doing yet. We are just not mature in order to be able to effectively manage the risks that we have and detect and deter any attacks.

We haven't had an audit as far as I know, a single entity pony up, and admit, "Yes, I had an intrusion that I defected into my SCADA Network."

I am having trouble believing that there is absolutely nothing going on in the SCADA Networks anywhere in North America that they are so secure that nobody has been to get into them. I am not buying it, but we are not detecting it and I have to think it is out there.

MR. DEWEY: I share some of Kevin's concern. The threat that I worry about the most, and it's the one that we have talked about the least, is the insider threat, the trusted employees that you

24 give access to the system after you have
25 done the requisite background checks and

1 validations and then we focus a lot of
2 our energy on the perimeter and who is
3 trying to get in as opposed to really
4 looking at what is going on inside the
5 applications and the data that maybe is
6 going out.
7 For that reason monitoring is
8 increasingly important, not only
9 monitoring your firewall logs which is
10 exceedingly difficult to do with the
11 volumes of data that you are talking
12 about, but also monitoring the internal
13 access to the applications and that data
14 validation is critical.
15 Kevin brought it up and somebody
16 else did too. You cannot assume that
17 the data is automatically right.
18 You have to pad some provisions in
19 there to validate that the data is
20 right, sort of an independent check not
21 only the data you are getting, but the
22 solution is right and increasingly these
23 applications are becoming more and more
24 complicated in terms of being able to
25 bulk those validation checks into it to

be able to detect those types of situations.

MR. DEWEY: The biggest risk or threat we are facing is also our biggest opportunity where it is simply the proliferation of modern technology systems and the complexity that is being built into the Grid around that.

There is good reason why we are deploying the technology because it is seed for streamlining operations in reducing costs that is necessary.

Obviously this is opening us up to the risk of cyber attack and we need to address that appropriately.

From a threat perspective, that's a very good question and I don't know that we know the answer.

As I visit utilities, I am asked often, "Who would want to attack us?" and particularly smaller entities they think they are immune from attack and perhaps they are.

I don't know that we understand completely what the motivations would be

and what the threats would be, but certainly the proliferation of technology is opening up risks even as it creates opportunities for us to improve the Grid and needs to be

addressed.

MR. FALKOVICH: I will mention two things in addition to everyone here.

There's an effort under the NERC CIP to identify the vectors of attack, to identify those risks of cyber attacks of the Cyber Attack Task Force or the cyber attack tree that is being built and that actually has the opportunity to identify a lot of these kind of entry by orders. To me one of the bigger challenges is not necessarily the attack itself but the response.

How is it a response to an incident? How do you share the information? How do we deal with the public and private partnerships with the government and industry?

In 2011, right, we had the first Grid exercise and that sharing had gaps

in it and PSE&G, our company was a very good player in this latest one in 2013 of GridEX II and we saw the communication flow much much more clearly.

We are seeing advancements made in this sharing of information, but I believe that there are still improvements that can be made to ensure

that the entities have the information quickly and are able to respond to threats in a quick and effective manner.

MR. WHITNEY: There are a couple areas to focus on. One is along the lines of awareness, so if we have a SCADA outage or a control system issue, can we effectively rule out that we know the attack pattern?

We know the attack signature to know that it wasn't a malicious compromise, truly a system failure sort awareness, that it was truly just a system failure of some sort.

It is an awareness around an understanding what the attacks are and

what the attack pattern will look like.

The other item is obsolescence.

Even though we have talked about embracing technology and interoperable systems capabilities that are associated with interoperability, we still have quite a few systems that are not interoperable that have reached end of life that vendors may no longer exist to provide support on those systems.

It does not necessarily mean that the bad guys don't know how to attack those systems or understand the vulnerabilities that might be present.

There still needs to be a considered efFort to help some of those folks that have reached end of life on their technologies to help them from the obsolescence perspective.

MR. PHILLIPS: Mr. Perry, you mentioned that integrity checking and hashing are not commonly being used in the bulk electric system right now.

Would you explain some reasons why you feel that is not occurring or there

are technological limitations, or is it just something people are not really focused on?

MR. PERRY: It just hasn't built into the systems. There is one EMS vendor that time stamps their data between the RTUs and the control center and they have to have satellite clocks to maintain accurate system time because of the time drifts between the two sites or the data transfer is rejected.

The other SCADA EMS vendors for the most part don't do that.

Time stamping data is something that has got to be built into the software that you are running, but the time stamping of the data prevents a replay attack.

19 If I can intercept your data and
20 even if I intercept your data in clear
21 text, I can't play that data back at a
22 later time because the time stamp is
23 going to catch it.
24 It's just something that we are
25 running on systems and even today EMS

1 SCADA systems are still using
2 architecture from pre-2000.
3 There has been a lot of work done,
4 but the basic concepts are the same.
5 It's the old adage, "If it ain't broke,
6 don't fix it," and the second piece of
7 it is, "Who's the first entity that's
8 going to step up and pay the vendor to
9 rewrite that system?"
10 That is not happening either and
11 it's an overlooked opportunity.
12 MR. O'NEAL: We have heard a lot
13 about the gaps and I do appreciate
14 everybody being up front about that.
15 We have heard about a consensus
16 really on objectives.
17 My question really is how do we
18 establish those objectives and then when
19 we do establish those objectives, how do
20 we determine if they are effectively
21 implemented and that could be anybody.
22 MR. SKAAR: There are a lot of
23 different frame works. The nice thing

about security frame works is that there are a lot of them to pick from. We just

have this missed one now.

That is a security framework that could work that has objectives.

Getting to the measurement point or determining whether you are secure or whether you are compliant with that security framework, the skill level required by the staff person particularly in the regions and at NERC needs to be at higher level in order to make those determinations because it is not a check in the box type of situation so the training that would be required, the qualifications required, and so forth, I have a saying, "We have to be at least as smart as the smartest registered entity that we have."

That's the skill level.

If we go down that path which, I think, is the path we need to go down, and then we transfer those objectives to map them over to the standards because we cannot keep reinventing standards.

We have to settle on them.

It's not a fair thing to do to keep

changing these things when we have so many folks involved in this industry.

We can get there with more training and more qualifications, but it does require the staff at the regions at NERC level to up their game significantly.

MR. WHITNEY: Something I mentioned during my opening statement was our implementation study where we are using the entities.

We are using the regional entities to work together to solve very specific technical compliance related issues and from the results of that what we are starting to see is a lot of out-of-the-box thinking on how they can apply the substandards to address dynamic and different things that are not that obvious to the substandards.

I would definitely encourage that type of approach where we have specific entities that we feel are going above the bar that can help us address issues that are more challenging.

MR. PERRY: There are two pieces of

it as Dan was saying. We have got to change our paradigm in how we develop standards.

Today we still have this need for

some reason to tell me how to do what I need to do. Be specific.

I don't want to besmirch any lawyers, but I would love to get the lawyers out of the room when I am talking security because lawyers deal in black and white and when you are talking about sanctionable enforcement the lawyers are going to be involved and they want to deal in black and white.

They don't want to deal in the shades of gray that cyber security is.

We have got to change our paradigm. I will give you an example that I used when I was vice chair of the Version 5 drafting Team a number of years ago.

Instead of telling me that I will use a username and a password and the password will consist of X amount of characters, certain complexity changed on a periodic basis, I want an objective

to assure the authentication of the individual for granting the individual access to my system.

One of them is very prescriptive and some systems will do it and some systems will not.

The other one is an objective.

We need to write objectives.

As Dan said, the people that come

in and evaluate whether the entity has achieved the objective we need step up our game.

I can only speak for the VBP regional entity, but every single person, everybody and myself, plus three staff on the enforcement team are certified information system auditors.

My lead analysts are also certified information system security professionals. It is not just book knowledge. You have to have real world experience.

I view auditing and everybody gets really concerned when I start talking about how I would like to audit.

I would like to come in and look at your controls.

If you're doing Sarbanes-Oxley, if you're doing SSA 16 SOC II type of audit, you have got controls.

You have got control objectives. You have got control statements and then you have got how you have implemented those controls.

My staff at least is perfectly capable of coming in, looking at your control objectives, your control statements, looking at protective, your

14 detective, your preventive and
15 corrective controls doing two things.
16 One is determining whether or not
17 you have implemented a reasonable suite
18 of controls to meet the control
19 objective, and two, have you effectively
20 implemented those controls and are they
21 effective in operation.
22 This is where we really need to be.
23 That way the entity can do what the
24 entity thinks is absolutely necessary,
25 and as long as the cat gets skinned, I

1 don't care how they skin it.
2 We just have to skin the cat.
3 MR. DEWEY: It is important to keep
4 separate the notion of security and what
5 makes us secure in compliance and what
6 makes us compliant.
7 They are both important.
8 We both strive very very hard to be
9 as secure as we can and as compliant as
10 we can and it seems like we spend a lot
11 more time in energy in worrying how to
12 be compliant as opposed to how to be
13 secure.
14 Tobias mentioned the RAI Program
15 and the need to develop the certainty
16 around how that is going to work and
17 having that assurances and that
18 certainty and those clear expectations

19 of how the auditing is going to be done
20 that will then sort of free up the
21 opportunity to then focus on, "Know I
22 what I need to do to satisfy that and I
23 focus on security," and the compliance
24 just falls out of that, so that is a
25 critical element for any of these

1 standards to be successful.
2 MR. PARKER: If we're going to take
3 an objective approach we absolutely need
4 to move away from pass fail audits.
5 I would suggest moving to a graded
6 assessment approach where an assessment
7 is made and a grade is given rather than
8 pass fail where you are rather poor, so
9 maybe it is an A through F or something
10 of that nature and identify your areas
11 for improvement.
12 We also need to move away from the
13 current approach where perfection is
14 required.
15 The analogy that I use often is
16 vector control where we are trying
17 mosquitoes or rodents or childhood
18 diseases, we do not seek perfection, we
19 do not try to eliminate everything.
20 We simply try to keep things down
21 and below an acceptable threshold and in
22 many areas of the standards we need to

take that approach as well and acknowledge that.

We may from time to time have a

vulnerability that gets exploited and we may have a successful compromise.

We need to make sure that the system does not fail. I am going back to Mr. Skaar's point earlier in looking at the systemic risk.

If we lose from an operating perspective, we can lose one transmission line. We can lose one generation plant.

From the cyber perspective, we need to be prepared to lose an asset here and an asset there, as long as the system is still resilient.

Moving away from past fail and moving away from perfection to more of an assessment based approach is absolutely critical to move forward on this.

MR. DeFALAISE: Before I start with my question, I want to thank you all again for coming down and taking your time to travel here. We really appreciate your attending and being panelists.

Mr. Perry and Mr. Parker both made references to some of their concerns about the fact that we have exempted non-routable SIR protocols.

In Mr. Perry's case he was mentioning that he has seen some of the entities that he has audited to prolong the use of a legacy approach for communication and then Mr. Parker mentioned that in some ESP there is not a routable protocol going on that is not necessarily falling into or the controls are not necessarily required to be compliant with that communication.

To the rest of the panelists, I ask, if at some point in the future a version set for consideration is given to the idea of removing the qualifier, a routable for the mandatory standards to apply to this communication protocol, i.e., it would not matter if it travels non-routable, it's just all communication would fall and meet that, what would be any of the adverse conditions that would arise by

eliminating the exception for the non-routable approach?

MR. FALKOVICH: What I would like to point out is that the current Version

5 Standards actually include serial communications, so when you talk about cyber systems at high impact control centers, at high impact facilities, serial is absolutely in.

In a lot of cases the communications in entities we are using is to go serial from the control center to the RTU, so they have to deal with it now.

You have to provide some sort of mechanisms for security under Version 5 Standards.

A lot of the perceived gap will be addressed with implementation of entities to meet Version 5 security requirements.

Similarly, I just want to raise the idea that serial communications in and of itself is very versatile. There are many serial types of communications.

I have a serial communication from the control center to the RTU, but I also have a serial communication from the RTU to somewhere else in the plant.

It is very tough to put borders around that conversation.

MR. PERRY: I will throw a couple thoughts in here even though I did raise

9 the issue.

10 Serial communication and routable

11 communication are two different beasts

12 and you don't protect them in the same

13 way.

14 The issue today with the CIP

15 Version 5 Standards, is it still taking

16 an outside in look?

17 There is language out there that

18 says that you only have routable

19 protocol if in the medium environment

20 which is where I think most of our

21 assets are going to be it is externally

22 reachable.

23 Well, a lot entities today think

24 that if they put a block in their

25 firewall to allow an inbound

1 communication request that that is good

2 enough.

3 I know the language was meant to

4 take advantage of unidirectional

5 gateways where you physically block

6 two-way traffic, but I am also telling

7 the enemies in the SPB region at least

8 that two-way communication externally

9 reachable can start from the inside

10 reaching out with TCP traffic it is

11 two-way, and once you have reached out,

12 then you have go two-way traffic and you

13 have the same vulnerabilities whether it

is a drive-by or fly-by type of issue or something else.

The problem we had with CIP Version 3 Standards is it was one size fits all.

If the data crossed the electronic security perimeter, there had to be an access point somewhere.

It's real tough to put in an access control point on a serial communication.

It doesn't make a whole lot of sense. There's not anything to authenticate. There's not a whole lot

there you can do.

If you focus on the data and protect the integrity and the availability of the data that is where you derive meaningful controls, that is, it doesn't make a difference whether it is serial or routable protocol.

Protecting how you get the data from Point A to Point B in one piece is where you need to set your control objectives and then you can do physical security controls where you have routable protocol you can certainly do your access controls, you can do your inbound and outbound like CIP Version 5 requires today for controls.

You can certainly do monitoring.

18 But you can even do monitoring on serial
19 if you pay attention to your SCADA
20 typology or your SCADA estimator, it
21 comes up, and says, "I have got some
22 data that is not making a whole lot of
23 sense here."
24 Do not blow it off. Investigate.
25 Find out why the data doesn't make any

1 sense.
2 It does not make any sense because
3 the RTU has gone south or is it not
4 making any sense because somebody has
5 hijacked the RTU.
6 In the end, it is the same thing.
7 You are getting bogus data.
8 Investigate the cause for the bogus
9 data and that would be one of your
10 control objectives. That is your
11 detective and your corrective controls.
12 MR. BARDEE: That concludes this
13 panel. We want to thank you for being
14 here and being so helpful in your
15 remarks today.
16 We will resume at one o'clock with
17 the second panel.
18 (Panel 2)
19 1:00 - 2:30 p.m. Need for Additional Definitions or
20 Controls for CIP Reliability Standards
21 Kevin Perry, Director, CIP, Southwest Power Pool
Regional

22 Entity

23 Richard Kinas, Mgr. Standards Compliance, Orlando Utilities

24 Commission

25 James Boone, NERC Compliance Manager, Pepco Holdings Inc.

1 Dr. Andrew Wright, N-Dimension Solutions

2 Andrew Ginter, VP Industrial Security, Waterfall Security

3 Solutions

4 David Batz, Director, Cyber & Infrastructure Security,

5 Edison Electric Institute

6 * * * *

7 MR. BARDEE: Welcome back everyone.

8 This is the time to start our second

9 panel for today.

10 The general top for this panel is

11 defined on whether additional

12 definitions and or security controls are

13 needed to protect BPS communications

14 networks, including remote systems

15 access.

16 One additional administrative

17 matter. I understand there were times

18 this morning when it may have been

19 difficult for the audience to hear one

20 of the speakers or questioners.

21 We encourage the panelists to make

22 sure that your microphone is turned on

23 when you're speaking and also to speak

24 loudly into it so we have no concerns

25 about people being able to hear you.

1 MR. PERRY: Good afternoon. My
2 name is Kevin Perry. I am the Director
3 of Critical Infrastructure Protection at
4 the Southwest Power Pool Regional
5 Entity.
6 Thank you for inviting me to speak
7 on the need for additional definitions
8 or controls for CIP Reliability
9 Standards.
10 While the CIP Version 5 Standards
11 represent a significant and positive
12 improvement in overall security of the
13 cyber assets supporting the reliability
14 of the bulk power system, there are
15 several issues of vagueness or outright
16 gaps that should be addressed.
17 I will briefly address each of the
18 significant issues in my opening
19 remarks.
20 First, the language of the CIP
21 Version 5 standards and definitions uses
22 the term "would," such as "would within
23 15 minutes," or "would affect."
24 I believe the language needs to be
25 prospective. From a risk perspective,

1 if something could happen, then entities

should assume that under the right conditions it would happen and require the protective controls be implemented.

The use of would implies certainty and registered entities may argue over that distinction in asserting certain BES Cyber Systems are not subject to the CIP Standards.

Looking at the definitions, a BES Cyber Asset is defined as a cyber asset that if rendered unavailable, degraded, or misused would within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed would affect the reliable operation of the bulk electric system.

While the definition of BES cyber asset appears to be precisely worded it is long, convoluted, and confusing.

The linkage of the cyber asset to the destruction, degradation, or

rendering unavailable of a facility, system, or equipment that in turn would affect the reliable operation of the bulk electric system when needed sets a bar that could result in not all BES Cyber Assets being identified.

The failure, misoperation, or even intentional operation of a BES cyber asset could potentially impact the reliability of the bulk power system without such extreme consequences being present.

The reference to affecting the reliable operation of the bulk electric system when needed is also problematic in that this condition is not clearly defined and is open to debate as to its meaning.

While I contend that an N-100 contingency might be when the proper operation of the BES Cyber Asset is needed, I expect that some registered entities may attempt to demonstrate the lack of impact through less comprehensive engineering studies rather

than assuming that there may be a scenario in which the proper operation of the BES Cyber Asset may be the only thing between BPS reliability and the initiation or furtherance of a cascading outage.

I suggest that a better definition might be one where the cyber asset is a BES Cyber Asset if it performs, supports, or affects the performance of

one or more BES reliability operating services and it does so in real-time currently defined as within 15 minutes of its required operation.

I am not as concerned about the fifteen-minute threshold.

Fifteen minutes may seem arbitrary and in some instances it may be hard to demonstrate, but it is based in operations and planning standards concepts and it is how the CIP Standard discriminates between BES Cyber Assets with real-time impact and those without.

Most cyber assets with real-time impact are expected to operate in far

less time than the fifteen minutes specified in the definition and are clearly BES Cyber Assets.

Similarly, many cyber assets without a real-time impact are also clearly non-impacting.

The interconnectivity of BES Cyber Systems remains an issue. I believe the CIP Version 5 criteria for categorizing BES Cyber Assets fails to address connectivity as instructed by Order 761.

The generator operator and balancing authority control centers are both subjected to an aggregate 1500 MW threshold to satisfy the minimum

criteria for identifying the control center BES Cyber Systems as medium impacting and subjecting them to meaningful protective controls.

Only the BES Cyber Systems of a transmission operator control center are unconditionally established as medium impacting if they do not satisfy any criteria making them high impacting.

Balancing authority control centers

and to a lesser extent generator operator control centers are directly or indirectly interconnected with each other and with reliability coordinator and transmission operator control centers through the use of ICCP which is the inter-control center communications protocol and possibly other protocols.

This interconnectivity spans BPS Interconnection boundaries, essentially exposing all of North America to the risk of compromise and misuse of the control center BES Cyber Systems.

To exacerbate the risk further at least one regional transmission organization, or RTO, has expanded its use of ICCP to include market participants that are not even subjected to the CIP standards.

The principles of mutual distrust are ineffective because the ICCP communications are necessary and must be allowed into the adjacent control center's network.

To minimize the risk, I suggest

that inter-control center communications, including ICCP, File Transfer Protocol or FTP, and web services be treated in a similar manner as interactive remote access.

Such access should be terminated in a DMZ outside of the ESP and the traffic into the ESP strictly controlled.

These protections should be required even for control centers containing low impacting BES Cyber Systems.

As I discussed this morning during the communication networks session, I believe that an appropriate subset of the CIP Version 5 Standards should be extended to the communication network infrastructure outside the ESP where the registered entity has administrative management control over the hardware.

While no one expects the registered entity to impose the CIP standards on a commercial carrier such as AT&T the registered entity can certainly apply

some aspect of the CIP Version 5

standards to the equipment it manages.

The Commission noted its concern in Order 791 with the uncontrolled use of transient devices within the electronic security perimeter and directed NERC to develop appropriate controls.

A standards drafting team is working on the issue now and I expect that basic security controls such as up-to-date patches and anti-malware will be required.

What I do not think is being addressed is the exclusionary language found in the definition of a BES Cyber Asset.

That definition declares "A cyber asset is not a BES Cyber Asset if for 30 consecutive calendar days or less it is directly connected to a network within an ESP, a cyber asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes."

I view a transient device as a

cyber asset connected to the network for

an express, limited, short duration purpose, and disconnected immediately upon completion of that purpose.

It should not linger on the network any longer than absolutely necessary and it should not be a device that is regularly and routinely connected to the network.

Under the current definition, I can envision a registered entity having a transient device that is continuously connected to the network for 30 calendar days, briefly disconnected, and reconnected for another 30 days, leveraging the 30-day timeframe to circumvent the application of more stringent cyber security controls.

Probably the greatest challenge one that is not addressed in the CIP standards is the rapidly expanding use of virtualization.

At audit, I am seeing virtual Local Area Networks defined in switches and routers where some VLANs are within the

electronic security perimeter and some are not.

I am seeing the deployment of virtual computing environments where the hypervisor is managing cyber assets

inside an ESP, perhaps even critical cyber assets, and cyber assets outside the ESP.

And I am seeing shared storage, typically large scale storage area network devices, again hosting storage for cyber assets within an ESP and for cyber assets outside the ESP.

These mixed trust environments pose a risk to the BES Cyber Systems running on them.

I am not opposed to virtualization, but I do believe that mixed trust should not be permitted.

The CIP Version 5 Standards need to clearly require Protected cyber asset treatment for the hypervisor and any virtual non-BES cyber system that is running on or can run on the virtual system.

The same should be true for any shared storage devices and a network device running Virtual LANs should either be an electronic access point with strong access controls or should either host ESP traffic or non-ESP traffic, but not both.

Another virtualization issue is the emerging use of cloud computing.

The CIP standards tangentially

address use of the cloud with the need to protect information about BES Cyber Systems.

The concern is beyond that however. There has been discussion about performing certain engineering functions including transmission planning studies in the cloud. What is to prevent real-time operations tools such as power flow, state estimator, and contingency analysis from being shifted to the cloud?

In the cloud the user loses control over the computing and storage resources being utilized and that gives me a

reason to be concerned.

Hopefully the definition of BES Cyber System and the application of the CIP standards to those systems are sufficient to discourage use of the cloud in support of control center operations. Only time will tell.

There are many more improvements that could be made to tighten up the CIP Version 5 Standards, but I will limit myself to the most important in the interest of time.

In summary, they are the use of would versus could in the standards and

definitions language.

The definition of BES Cyber Asset.

The issues around interconnectivity especially through the use of the ICCP protocol.

Critical communication network equipment, transient devices, and the rapid growth in the use of virtualization.

Thank you for the opportunity to provide opening remarks for this

technical conference and I look forward to the discussion to follow.

MR. BARDEE: Thank you, Mr. Perry. Next up we have Richard Kinas, manager of standards compliance for the Orlando Utilities Commission.

MR. KINAS: Yes, thank you, and good afternoon. My name is Richard Kinas, I am the manager of Standards Compliance for Orlando Utilities Commission.

Thank you for providing me the opportunity to address this important topic.

Version 5 of the NERC CIP Standards is a substantial move forward by industry and government to require protection for the bulk electric system.

In support of this effort FERC in

its oversight position has a asked is there a need for additional definitions or controls for the CPI Standards?

the Federal Power Act defines the term cyber security incident as a malicious act or suspicious event that

disrupts or was an attempt to disrupt the operation of those programmable electronic devices and communication networks including hardware, software, and data that are essential to the reliable operation of the bulk power system.

The definition clearly differentiates between programmable electronic devices and communication networks.

Therefore, it is definitely appropriate that the standards differentiate as well.

Communication networks are the underlying infrastructure that provides remote access as well as a path for transferring data or information required to operate the bulk power system.

The data information and remote access functions are what is critical to operating the BPS. The communications

networks are simply the current technology that allows these functions

to occur.

It is the functions therefore remote access and data information transfer that must address confidentiality and integrity while availability is most appropriately addressed by the underlying network communications infrastructure.

The creation of any new standard must address the availability requirements of communications networks as well as the confidentiality and integrity requirements for data, information, and control traversing those networks.

Specifying requirement for protection of data information and control traversing communication networks must be based on the amount of risk each of these different types of data information and control posed to the BPS if either lost or compromised.

Real time power flow data associated with boundary point tie lines of a balancing authority required to

calculate ACE is much different than watt hour meter value being sent to a TOP for after the fact billing true ups.

In this case the BA data is required according to a reliability standard while the TOP data is not.

It must be the specific value of the data to perform the required reliability function that governs the security controls required however, even if some data or information is required by reliability standard such as a dry contact copper connection from a substation switch yard to an RTU within the substation control house to send a reactive resource status indicator the confidentiality and integrity requirements must be carefully considered to evaluate if they are warranted at all.

The standard should clearly identify the expectations related to each type of data for information based on its impact to both power system operations if lost or compromised.

Controls need to be established to provide for remote access but a remote user establishes remote access they become a part of that system for the duration of the connection.

That means the system now extends to the remote location. The strengths and weaknesses of the remote users infrastructure becomes the strength and weaknesses of the system itself.

Controls must be put in place to be able to monitor and manage the remote access in real time and terminate if the access exceeds a predetermined risk threshold.

Thank you.

MR. BARDEE: Thank you, Mr. Kinas. Next, we have Mr. James Boone substituting for David Becker from PEPCO Holdings.

MR. BOONE: Good afternoon members of the Commission and Staff.

I am James Boone, manager of strategic initiatives at Pepco Holdings, Inc., PHI.

PHI is one of the largest energy delivery companies in the Mid-Atlantic region serving approximately 2 million customers in Delaware, the District of Columbia, Maryland and New Jersey.

My remarks speak to whether additional definitions and security controls are necessary to protect bulk electric system, communication networks

including secure remote access to control and monitoring devices.

These remarks commend the industry for making significant advances in the area of cyber security fostered by the North American Electric Reliability Corporation Critical Infrastructure Protection Reliability Standards.

NERC CIP Standards require information protection and adequate security practices to protect the reliability of the BES.

It is my understanding at some utilities outside of North America are choosing to voluntarily comply with these standards.

The NERC CIP Version 5 Standards continue to drive proven security practices to support the reliability of the BES.

In this pursuit utilities are addressing technical challenges and dedicating resources to advance the security and reliability of the BES.

The industry is actively identifying the facilities and assets to be covered and classified under the NERC CIP Version 5.

A stability set of standards is the best environment to enable business to

drive mature processes.

BES communications networks are usually complex private networks with large capital investments connecting numerous field sites with control centers. They have been designed with redundancy and high availability requirements.

BES networks and systems that depend on field asset data often have integrated monitoring to further support

reliable operations and adding compliance layers to these high availability networks would serve mostly to increase cost and network complexity.

Ensuring effective definitions are in place is essential.

The latest version of the NERC glossary of terms is missing some key cyber security and communications definitions.

Terms like end-to-end encryption, authentication, authorization, and identity services are important to robust cyber security and communications programs.

It is important that cyber security terms are defined so that a common understanding of the terms can be

established.

Many cyber security terms are already defined in the National Institute of Standards and Technology Interagency Report, NIST IR 7298 and this document may be referenced as an approved definition source for future

NERC guidance.

Terms that are specific to NERC CIP should be defined in the documents and definitions should not be duplicated that are already defined in NIST IR 7298.

The cyber asset definition for example references the term programmable electronic device which is very broad and could actually distract from the identification of key digital assets that secure the BES.

The revised definitions change as the revised definition of the physical security perimeter correctly shifts the focus away from the six-walled boundary concept to controlled access areas.

In Version 5 it also removes references to computer and telecommunications rooms which may lead to missed communications system protections.

Entities are perceptive to maintain

a supplemental glossary of terms specific to their compliance department

and PHI has one as well.

Protecting access to critical non-routable assets within a cyber program is challenging.

Entities are prudent to document all connections to essential cyber assets, including dial-up and non-routable devices.

These connections are then described on the ESP, electronic security perimeter drawings.

NERC CIP Version 5 requires strong authentication of dial-up connectivity.

Mature cyber programs secured non-routable links especially that extend to multiple network segments.

Critical cabling within an ESP already receives the protections of a PSP.

To further manage risks, entities must consider protection methodologies for key local communication control systems and related cabling.

As mentioned previously, PHI internal communication networks offer

high performance and high availability communications networks.

Given the reliability of these communications technologies and redundancy design into these systems, the core cabling should remain outside the scope of the NERC CIP standards.

End points of these communication links are already in scope as they become access points into ESPs which have effective security requirements.

Under NERC CIP Version 5 secure remote access to cyber assets requires authentication, authorization, and access privileges.

NERC CIP Version 5 requires a dedicated asset outside of the ESP sometimes known as the jump box to provide the trusted platform to connect to the cyber assets within the ESP.

This model ultimately provides flexibility and strong security.

NERC CIP Version 5 is mostly silent on securing data in motion across the network.

Access is strictly controlled at the electronic access point and using identity services at the device.

In addition to access controls

utilities may further reduce risks by using standards-based encryption and active monitoring services like intrusion detection systems, network access control systems and anomaly detection to address unusual network traffic.

Encryption provides another layer of protection for securing the data. However, as encryption methods are selected many items need to be taken into account.

Encryption adds latency to the transmission of data. Many of the end devices do not yet support internal encryption and while encryption obfuscates the message from intruders it also introduces complexity into device-to-device connections and most monitoring systems.

PHI will continue to work with

utility asset vendors to enhance their products to support security protections.

Targeted system replacements and upgrades will support security and compliance initiatives.

PHI will continue to seek to improve its services which automate identity, access, encryption, monitoring

and alerting systems.

The NERC CIP Version 5 reliability standards we believe together with PHI's security architecture will continue to drive strong security practices into the PHI's BES.

Appreciate the opportunity to participate today and the opportunity to provide these comments.

MR. BARDEE: Thank you, Mr. Boone. Next, we have Dr. Andrew Wright from N-Dimension Solutions.

Dr. Wright.

DR. WRIGHT: Good afternoon, Commission members, thank you for the opportunity to address you and just for

background I am the chief technology officer of N-Dimension.

We are a vendor of solutions and products for utilities security.

I am speaking to you in my capacity as a concerned US citizen today.

The Version 5 CIP Standards contain no requirements for encryption or authentication of critical control signals such as SCADA commands, whether those signals are carried over IP connections, or serial or even the public Internet.

You can route your SCADA through Moscow and every Starbucks along the way and you are CIP compliant.

Most major Internet businesses such as Google Mail, Yahoo Mail, Facebook, Twitter, Skype, et cetera are moving to adopt encryption for all communications between their users and the services but also for traffic between their data centers internal traffic within their operations.

While their motivations are

different the threats that are driving these businesses to adopt encryption apply equally to the networks that carry controls signals for the power grid.

An increasingly sophisticated set of hardware and software exploits is available to potential attackers.

Exploits are available for both IP and serial communications.

Physical access to communications paths whether fiber, microwave or other is not difficult to achieve due to the geographically distributed nature of the power grid communications networks, hence a private nature cannot be relied on to provide security.

Strong cryptography is the only viable means of ensuring the

19 authenticity and integrity of control
20 communications across that diverse and
21 distributed network and protocols,
22 applications, and products are widely
23 available for encrypting IP links.
24 Most modern processors contain
25 hardware support for cryptography

1 enabling the implementation of
2 cryptographic operations with its
3 minimal impact on communications.
4 That includes Intel processors such
5 as in my Mac. It also includes ARM
6 processors such as in my iPad.
7 However, a substantial portion of
8 control center to substation
9 communications still uses slow serial
10 links.
11 The challenge to encrypting serial
12 links is not in computational capacity,
13 but in additional overhead added to the
14 slow communications line.
15 Between 2004 and 2008, American Gas
16 Association Working Group 12 developed a
17 cryptographic protocol specifically for
18 the purpose of assuring the integrity of
19 serial communications.
20 I was a key technical contributor
21 to that protocol.
22 The protocol is intended to provide

retrofit protection via bump-in-the-wire link encryptors.

The protocol was implemented by

about a half dozen manufacturers and their prototypes were tested for interoperability against a reference implementation which is available as open source written by me.

Subsequently the protocol was transitioned to an IEEE standard and is now known as IEEE 1711, cryptographic protocol for cyber security of substation serial links.

Unfortunately, this protocol saw little market uptake and most of the implementations that were built now appear dormant.

Similar to IEEE 1711, DNP3 Secure provides cryptographic authentication for the DNP3 SCADA protocol which is widely used for substation communications in the US.

DNP3 Secure can provide authentication for both IP and serial DNP3 links.

Yet another protocol is available to encrypt transfer trip and substation to substation protocols that control

tripping of breakers.

Those are the kinds of protocols we have heard about earlier to day that require one second latency devices to encrypt communications have been available for over five years.

Given the availability of the protocols and albeit minimally deployed hardware products, FERC could consider mandating the implementation across the serial links of the power grid.

An upcoming mandate would then drive the development of products and make those products available to utilities. But the specialized nature of these devices would make them expensive and a full roll out across the grid would leave utilities even more locked into outdated 20th century serial technology.

There is a better way.

The current CIP standards include a variety of exclusions to compliance requirements for cyber assets and sites that are connected solely by

non-routable protocols being largely serial links.

These exclusions do not exempt serial links from encryption since there

is no encryption required for any kinds of links.

However, these non-routable protocol exclusions are in part responsible for utilities retaining serial links and we have heard several examples of that already today.

In once case that I encountered utilities removed IP links in order to simplify their CIP compliance efforts.

CIP Version 5 had made changes in this area that make it I would say a little muddier as to what is going to be excluded by the non-routable protocol exclusions but there are still a substantial number of exclusions there.

Therefore, as Version 5 is adopted most utilities will likely retain their serial equipment.

Eliminating the non-routable protocol exclusions would not directly

force deployment of encryption for control traffic.

However, by removing this incentive to stick with serial communications the ever decreasing costs and increasing capabilities of IP-based networking equipment would likely be sufficient to motivate utilities to modernize their

9 communications networks.

10 Network vendors now have devices

11 that communicate routinely at 10

12 gigabytes and 100 gigabytes is very much

13 on the way and even being deployed.

14 This is a million times faster than

15 the typical substations serial link.

16 With encryption mechanisms

17 available in networking and substation

18 equipment, even in those high speed

19 links security protocol such as IPSEC

20 and SSL could be implemented at minimal

21 additional cost as modernization of the

22 power grid communication network

23 proceeds.

24 Switching to IP-based high-speed

25 communications will have other benefits.

1 These networks will enable access

2 to high resolution stranded data that is

3 generated by modern substation

4 equipment, but too large to be retrieved

5 over slow serial links.

6 High-speed connections will also

7 better support development of or

8 deployment of synchrophasor measurement

9 units which generate larger volumes of

10 data.

11 IP-based communications can support

12 many other applications such as

13 electronic locks and video surveillance

and new applications that have yet to be conceive.

Finally, IP-based dynamic routing can reroute substation communications across multiple paths, fiber, radio, satellite and could potentially provide more reliable communications not only during accidental outages but also possibly during attacks.

Compliance requirements for encrypting control traffic may also be necessary, but it is my opinion that

removing the incentives for sticking with outdated serial technology will go a long way towards driving adoption of encryption.

Thank you.

MR. BARDEE: Thank you, Dr. Wright. Next we have Andrew Ginter, vice president of industrial security for Waterfall Security Solutions.

MR. GINTER: Thank you Mr. Chairman and my thanks to everyone here for the opportunity to address you.

I represent Waterfall Security Solutions. Waterfall is on record expressing concern about the security of central turbine monitoring systems and other kinds of interactive remote access

and control systems in the cloud.

We are on record in submissions to the NERC Reliability Impact Steering Committee and in comments to the FERC process approving the NERC CIP Version 5 Standards as well as other venues.

Let's take the concrete example of turbine monitoring systems.

Most turbine vendors will not provide a site with a turbine hardware support contract or with a hardware warrantee unless the site permits the vendor to continuously monitor the turbine and to occasionally adjust the turbine remotely.

The vendor may monitor for vibration anomalies or for heat distribution anomalies or they may monitor the control system for other things.

The vendor monitors with their expert people and with their expert systems from a central site. They look for small anomalies that could grow into premature catastrophic failures of the rotating equipment or of the control system.

When an anomaly is found - typically several times per year - the vendor's central site reaches into the

turbine control system and adjusts parameters to correct the anomaly.

These are called monitoring and

diagnostic services.

To facilitate these services, turbine vendors generally establish encrypted virtual private network or VPN connections from the vendor's central monitoring site into the generating entity's control system network generally bypassing all of the entity's corporate security technologies in the process.

Even when the vendor has sold a monitoring and advice only service with no remote control the VPN connections and the associated security technologies are often set up identically.

They are set up to provide the turbine vendor with continuous remote control no matter what service the vendor has in fact sold to the site.

What this means is that there is only one layer of security between any monitored turbine anywhere in the world and any other monitored turbine anywhere in North America.

Any attack from any one compromised

generating site however sophisticated or unsophisticated the attack, whether that compromised generating site is in a geography where NERC CIP is in force or not, whether the compromised site is CIP compliant or not, any attack that breaks through that one layer of security, into the vendor's control center that attack gives the attacker remote control of hundreds of very similar targets.

So let's think about this. The continuous interactive remote control permissions that generating sites grant to these turbine vendors, these permissions are much more intrusive than are the ICCP set point permissions that generating sites routinely give to CIP-regulated balancing authorities and other BES Control Centers.

In spite of these more intrusive permissions NERC CIP currently requires no technical security measures of the central vendor sites.

Now, for vendor personnel with remote access to generating sites CIP

does require background checks and training and awareness programs.

Nothing in NERC CIP, though,

requires any technical security controls for the turbine vendors.

There is a solution to this problem that some entities have implemented. Some entities are deploying hardware-enforced unidirectional security gateway technology and remote screen view technology.

The gateways put copies of plant data sources on to business networks across hardware-enforced one-way communications channels.

The gateway hardware prevents any network attack from compromising the protected site.

The gateway software produces faithful real-time copies of turbine computers and turbine data sources.

The turbine vendors' central sites and expert systems monitor the copies. The copies are accurate enough that the vendors' systems all still work.

The vendor personnel often have no idea that they are working with copies.

When turbine adjustment is needed though the vendors figure things out fast.

No signal they send can penetrate to the turbine networks to adjust the turbines.

So what they have to do is they have call the site and the site turns on screen sharing via remote screen view.

The technology sends real-time screen images through the one-way hardware so that the vendors can see what is on the screen of an engineering workstation on the protected control system network.

The vendor can give advice over the phone to the people at the turbine site. The vendor can watch as the personnel at the site use the engineering workstations to correct problems.

With unidirectional gateway and remote screen view technology no attack on a turbine vendor's site however

sophisticated can propagate to unidirectionally protected sites.

Waterfall's concerns regarding central computing and diagnostic systems really reflect a deeper concern about interactive remote access from any one site or from any one laptop to large numbers of similar targets in the BES.

Individual remote access is a problem, yes, but the really big problem is control system vendors, turbine vendors, and the most senior of

generating entity support personnel.

Each of these vendors and each of these senior personnel may have access to hundreds of VPN tunnels to hundreds of CIP-critical sites simultaneously.

These cloud-based diagnostics systems and these senior support personnel all represent extremely attractive targets for cyber attacks.

It's my understanding that these risks have been assessed by different parts of NERC and have not yet been found to merit any action.

Waterfall respectfully disagrees in this assessment. We do not believe that it is wise to rely on a single layer of security to protect the reliability of large numbers of similar targets in the bulk electric system.

Given our discussions with many entities and with vendors as well we do not believe that entities generally or vendors generally, although there are exceptions, are seeing this threat as a serious one or that they are taking appropriate measures to mitigate the threat.

We encourage FERC and NERC to address this threat to the reliability of the bulk electric system.

This concludes my prepared statement.

Again, I represent Waterfall Security Solutions and for the record Waterfall is a technology provider.

We produce and sell unidirectional security gateways and stronger-than-firewalls technologies.

Thank you for listening.

MR. BARDEE: Thank you, Mr. Ginter. Finally for this panel, we have Mr. David Batz, the director of Cyber and Infrastructure Security for the Edison Electric Institute.

Mr. Batz.

MR. BATZ: Good afternoon Mr. Bardee, and members of the Commission staff. My name is David Batz, Director of Cyber & Infrastructure Security at Edison Electric Institute and I am here today representing Edison Electric Institute and its member companies.

We appreciate the Commission holding this conference.

EEI member companies are strongly aware of the importance of reliability to our customers and there fore the importance of the issues that we are covering today.

Protecting the nation's electric grid and ensuring a reliable supply of energy is the electric power industry's top priority.

The industry takes cyber security threats very seriously.

Cyber security incidents may disrupt the flow of power or reduce the reliability of the electric system.

Key to the success of this effort is the ability to provide measures capable of protecting the evolving intelligent network against interruption, exploitation, compromise or outright attack of cyber assets whether the attack vector is physical, cyber, or both.

Our members are committed to providing reliable and resilient infrastructure for the communities that we privileged to serve.

We believe that reliability consists not only of protection and prevention, but also recovery and response.

We believe that entities need to have the ability to be flexible in responding to evolving and newly emerging threats.

Recognizing that there are a broad range of interdependencies and potential consequences associated with the loss of different facilities or components, EEI supports a risk-based prioritized approach that identifies assets truly critical to the reliable operation of the electric grid.

This ensures that the most important elements of our system receive the highest level of attention as well as the resources necessary to secure them.

Without engaging on the specifics of potential vulnerabilities associated with the equipment that is the subject of this technical conference it is important to consider that bulk power system owners and operators have to evaluate and prioritize relative risk on a constant basis and that the range of threats and vulnerabilities have widely varying potential impacts on the system.

Protections provided for a specific asset should be commensurate with the

associated cyber or physical risk.

Further, the controls established for a specific equipment need to be

assessed as part of each entity's defense in depth of all of its BES cyber-systems and not in isolation.

In response to cyber and physical threats electric companies employ various strategies to protect these systems, but security risks still exist to some degree.

With respect to the issue of changes to the NERC Glossary of Terms, EEI believes that it is appropriate for the structure of the mandatory CIP standards to arrive at a steady state.

As a general matter, EEI strongly believes that the Version 5 NERC Standards ensures a durable and long-lived framework that allows companies to decide most appropriate technologies, applications, and controls based on risk assessments of their assets and facilities.

Technical discussions of new and

emerging issues can and should take place in a far more productive and efficient venue other than the NERC standards development process.

In addition, EEI believes that considerable process exhaustion has taken its toll on stakeholders in the

Version 5 Standards development.

Considering the highly dynamic nature of CIP and cyber security issues and evolving technology, EEI urges the Commission to allow time for companies, NERC, and the Commission itself to gather experience with Version 5 and continue discussions on the technical issues in appropriate industry venues.

In the near term as the industry embarks on Version 5 Standards compliance activities and NERC and the regions develop associated audit and compliance review materials, EEI suggests that guidance documents addressing specific technical matters incorporate particular appropriate terms and definitions such as those published

in NIST IR 7298.

Although there are a number of physical or logical controls that can be employed to protect BPS communication network components communicating via non-routable protocols or through serial communication links there is no silver bullet to address all potential communication related cyber security problems.

Entities may employ physical security mechanisms to aid in the

protection of remote nodes in addition to the practice of physical security often used to protect central collection communication servers.

Recognizing that physical security cannot be guaranteed particularly for remote unattended facilities entities may incorporate other controls as part of an overall risk management strategy.

These may include integrity checks and out-of-bounds detection for communication links as well as working with system vendors to understand how

their products respond to invalid or unauthorized messages being inserted into a communications channel.

Some entities may choose to incorporate cryptographic modules for certain serial communications.

However, it is important to remember that encrypted serial communications does not solve or address all potential attack vectors.

In addition there are important availability and performance issues that should be contemplated before cryptographic modules are deployed.

As specified in the PNNL AGA-12 Part 2 performance test results

discussed earlier, and I will just read a couple of outtakes from the report.

Reliable operations of vendor equipment will directly impact the willingness of asset owners to adopt any technology.

In addition, an installed security appliance that is inoperable provides no added value to the field device.

Finally, security solutions cannot adversely impact reliable operations or personal safety.

Although there are a number of physical or logical controls that can be employed to protect non-programmable components of data communications networks such as cabling, there is no single solution or technology to address all potential communication related cyber security problems.

Each entity should consider the facts and circumstances associated with communication paths that are used for BPS related communications.

These measures can include restricting logical access to the network and network activity restricting physical access to the network and network devices protecting individual components from exploitation maintaining

22 functionality during adverse conditions
23 and restoring the system after an
24 incident.
25 The particular measures selected by

1 an entity to manage risk associated with
2 communications networks are dependent
3 upon a risk assessment and an
4 understanding of the BPS process to be
5 secured as well as the features or
6 limitations of the network media,
7 equipment, and interfaces as well as
8 health and safety considerations.
9 In addition it is important to note
10 that the use of encryption can
11 significantly complicate the
12 implementation of other security
13 controls such as intrusion detection
14 systems and anomaly detection systems.
15 Regarding the types of physical or
16 logical controls that may be needed to
17 address the cyber security needs of
18 remote access processes and devices
19 Version 5 brings a strong set of new
20 requirements and controls for remote
21 access.
22 The next two issues securing data
23 in motion and questions about encryption
24 will be addressed together.
25 As stated earlier the particular

measures selected by an entity to manage risk associated with communications networks are dependent upon a risk assessment and an understanding of the data to be secured as well as the features or limitations of the network media, equipment, and interfaces, as well as health and safety considerations.

Encryption does not solve all security problems, and if improperly implemented can lead to a lack of availability and reliability.

As mentioned in a prior panel, the Department of Homeland Security guidance does recommend that entities be careful about the use of encryption recognizing the potential for them within appropriate encryption techniques to create a self-inflicted service attack.

This obviously does not lead to enhanced reliability.

Cyber security risk as with all risk cannot be completely eliminated, but instead must be managed through

informed decision-making processes.

EEI member companies are committed

to maintaining the safe and reliable operation of the BPS and managing the cyber security risk.

Mandatory and enforceable standards represent an important tool that can be used to support the reliability of the BPS.

However, standards alone are not sufficient to address a dynamic environment of the emerging risks, unpredictable threat actors, and rapid changes in technology.

The industry is also engaged in public-private partnerships, information sharing between government and industry and exchange of best practices both within the electricity sub-sector and with other critical sectors and disciplines.

Thank you for the opportunity to provide this statement and I would be happy to address questions that you may have.

MR. BARDEE: Thank you Mr. Batz, and thanks to all of you. Let me begin with just a couple of questions.

One has to do with the network between EPSs, connections between the ESPs.

In your statement earlier this

morning, Mr. Perry, you suggested that there should be some type of controls for those connections within an entity, if an entity controlled the connections between ESPs, you suggested that there should be some responsibility to protect that in some way. Can you go into more detail about that?

MR. PERRY: Certainly. What I said this morning and alluded to in my opening statement is that the current substandards explicitly exclude all communication infrastructure outside of the ESP and that includes data communication paths between ESPs or between an entity's field assets and the control center, for example.

What I offered was that there

really are two types of communications infrastructure in play here.

There is infrastructure that is owned, managed, administered by the entity, and there is infrastructure that is commercial carrier.

If you own the routers and the switches outside of your ESP up to your border, and you manage them, you should be able to protect them. They are yours.

12 The commercial carrier, the AT&T
13 fiber stack, can sit inside your
14 physical security perimeter, but you are
15 not going to manage it from a cyber
16 electronic perspective.
17 That is AT&T's equipment.
18 But it can sit physically
19 protected. There are some controls you
20 can do there.
21 Once it leaves the physical
22 premises of your building and hits the
23 wide area infrastructure that the
24 commercial carriers have put into place
25 it is outside of your control.

1 You cannot do anything about it
2 until it gets to the other end where,
3 once again, you regain control over the
4 infrastructure that that communication
5 is pathing over.
6 The gap I'm pointing out is the gap
7 between your ESP border and your
8 communications border where you maintain
9 control.
10 I am not necessarily advocating
11 that every bit of that equipment be
12 subjected to 100 percent of the CIP
13 Version 5 Standards, but certainly there
14 needs to be something more than, "Don't
15 worry about it."
16 MR. BARDEE: Mr. Boone, in your

statement you described some of the cabling within your company. Do you have a reaction or thoughts on the approach that Mr. Perry just described or if other witnesses do?

MR. BOONE: Thank you for the question. We have our private communications network internally, so we certainly have the protections

end-to-end, and if I understood the concern, it is when it goes out on to a third-party system.

I may have understood that.

But we have the end-to-end point, so from the substation to the control center, or substation - substation, we have what controls are in place to protect that information when it is received because it is within our facilities, so I mean we do have some physical controls as well with the facilities located at the substations both the communication and the equipment on both ends of that.

With respect to the cabling and the physical controls on the cabling there are limitations. There could be a lot of fiber optics, for example, cabling across the system.

We can put in some protection equipment to detect if somebody is impacting the cable through a shielding, and whatnot, but that is a costly proposition.

If I understood the question right, the third-party side is not something that we're as concerned with because with our own private networks we think we have the controls on the ends and certainly we have as much physical control as we can to protect the cabling.

We also have redundancy, the resiliency issue. We have redundancy. We have communication that goes into a black box as long as you can get the data into that box. There are multiple ways it can come out.

We have that built into our system as well that you want to balance when you are looking at the various controls for the communications.

I don't know on the one third-party side if that is equally applicable, but we certainly have redundancy built into our system.

MR. BARDEE: For the assets and the equipment that you only control, do you think it is appropriate to have

requirements ensuring that kind of protection?

MR. BOONE: We think that Version 5 strikes a very good balance and I would agree with EEI that we would prefer to see stability with these standards and gain the experience.

We have not had issues with our communications network, so I don't think additional protections are necessary for us beyond what is in Version 5 right now.

MR. KINAS: If we take a look at all the infrastructure that is outside of our ESP, whether it is company owned, or whether it is carrier owned, or some other party, it can affect the availability of the data.

But we need to ensure that the data -- well, the only reason that we are concerned about putting controls on the devices, if we own them, is because we might see if we have the ability to transfer that data unencrypted, but as long as that data leaves encrypted from

our site, it doesn't matter whose latent ESP, it does not matter whose particular

infrastructure it is riding across, it will not be protected.

We do have availability concerns at that point. If the equipment has no controls on it, then we could have a hacker that could get in and affect the availability of that data and its transport.

When we look at it control would be good to address some of the availability concerns, but not as far as the compromised or integrity concerns.

MR. BARDEE: Dr. Wright, in your statement you talked about the exclusion for non-routable protocols, and if I understood it right, you were suggesting that we should eliminate those exclusions so that people had incentives to shift more towards IP based technology.

Could you talk about that a little bit more and then I am sort of assuming that at least one or more of the other

panelists might question that position.

DR. WRIGHT: We know that we have a lot of older serial communications in the power grid today.

I have spent a good number of years working on that AJ12, now IEEE 1711,

protocol trying to figure out to encrypt that with minimal impact.

Other folks have built similar protocols. It is possible to do that.

However that locks us into this old technology, and honestly, the 1980s or older technology, 1966 baud serial links.

If we can instead move to IP-based communications, yes, there are different challenges with IP-based communications but there are a whole lot more benefits that come along with those communications.

The economics make a whole lot more sense. Ultimately, we may be spending around the same number of dollars to protect the older serial stuff than to replace it with modern equipment.

Let's spend it on the modern stuff and get on to the applications that can vent the grade a whole lot more.

Encryption is one of the things that is reasonably straightforward and well known how to do in the IP world.

MR. BATZ: I agree that IP routable technology provides a lot more in terms of the sort of feature set.

It is important to remember that there are a number of substations and

12 facilities that are located across North
13 America that have extremely limited
14 telecommunication facilities that are
15 available to them at a reasonable price
16 point.
17 It's sort of a false option to say,
18 "I can either use a 9600 baud old
19 fashioned serial communication or I can
20 use a multi-gigabit high-speed link."
21 Now, "Think, think, think. Which
22 one do I want?"
23 In many cases the high-speed link
24 is not an option. It may be in some
25 cases, but it is important to also

1 consider, frankly, the voice of the
2 consumer and the voice of the state
3 regulator who is very concerned about
4 passing certain costs on to the end
5 consumer for these services.
6 MR. GINTER: I just wanted to add a
7 point. I have heard in the course of
8 the day here a great deal of discussion
9 of encryption and the alternative here
10 is IP plus encryption versus serial.
11 I wanted to point out that
12 encryption, yes, it buys you a degree of
13 protection against man in the middle
14 attacks.
15 Encryption buys you nothing if an

end point is compromised as would be the case if you have a compromised laptop with connections to hundreds of sites or if you have a compromised vendor control center. That was the point I wanted to make. Thank you.

MR. PERRY: A couple of points. I want to go back one question and just clarify.

When I am talking about protecting

the infrastructure beyond the ESP, I'm not talking about cabling.

The Version 3 Standards with the six-wall boundary expectation on a data cable were very problematic, and of course, it never envisioned the possibility that you might want to communicate with something other than physical media like wireless.

You still have networking equipment, cyber assets, and it is the cyber assets that you are controlling and you are maintaining and you should be protecting.

The CIP Version 5 Standards have relaxed, the six-wall boundary issue, you now have layers of protection and the cabling is not a six-walled boundary issue anymore, so I am not too concerned about that.

Serial versus IP, I agree with what Mr. Batz said. You don't have high-speed Ethernet out in the middle of absolutely nowhere where some of these substations are.

You are lucky to have four-wire twisted pair running 1200 baud. You just cannot do anything.

But I have also seen entities that have converted back to serial communication because of the CIP Standards.

I have actually seen an RTU with an IP address label still stuck on it and the RJ-45 cable hanging next to it clearly communicating with a serial protocol.

Why? Because if it communicated with a routable protocol it was a critical cyber asset and the entity could not have that.

I have seen entities upgrade their systems, the remote control of a Black Star generator, and because the new system communicated with IP, they now jump in a car and they drive out to the Black Star unit to start it rather than remotely starting it because under the new protocol, under the new system, it

would communicate with a routable

protocol and all of a sudden they would have stuff that were critical cyber assets.

It is that disincentive that we need to address and not mandate that IP traffic go to every single substation generating plant in North America, but we have to deal with this preoccupation of managing the risk of noncompliance as opposed to managing security.

MR. BARDEE: One of the themes that we heard then, as you have just described it, and I have heard in other contexts before today is that regulatory efforts often have an unintended consequence of incentivizing the exact opposite behavior.

But nonetheless we have an obligation to have requirements and hopefully we structure them in a way that elicits good behavior, meaning, positive change, beneficial change.

If any of the other witnesses have suggestions on that, I am very open to those ideas.

MR. BATZ: I appreciate

Mr. Perry's last statement about tension. There is a tension between what I will call "compliance liability" and really "security liability."

It is simply important for everybody involved in the discussion to recognize that at the end of the day there is a finite pool of resources available to address risk whatever the risk is.

It is physical, cyber, compliance, security, there is a finite set resources available.

To the degree that there is an opportunity for what I will call a robust discussion between regulated entities and the regulator or regulators in the case of the North American system let's talk about managing risk, not eliminating a risk, but in actual discussion about managing the associated risk.

The problem is such discussions in order to be effective must consider the

facts and circumstances that are associated with not only the entity of which there is a bunch that fall under the mandatory compliance regimen, but within their facilities, they have, it is not hundreds, but generally thousands

or hundreds of thousands or more nodes that each have some type of attack surface potentially and each of which offer an important service to that entity in its pursuit of reliability.

There are not easy answers even though everybody wants to find the silver bullet, but one silver bullet is out there.

MR. BARDEE: For the next panel, when they come up, I will ask them to come with the "easy answers."

MR. PHILLIPS: Several panelists mentioned potential gaps in the standards relating to some of the exceptions with respect to remote access.

Let me put this out to everybody.

How strong do you all feel that the

remote access protections are in the Version 5 requirements and is there anything in your view that we would need to do to make them stronger even compared to relative other frameworks that are available?

MR. PERRY: I will start and we can work our way down the line. Weak as water. Here's the problem.

We are requiring a jump host. That

11 is great. But if all I have to do is to
12 strongly authenticate onto a jump host,
13 and then I can remote desktop, BNC,
14 Telnet, SSH, FTP, pick your poison, from
15 the jump host through the firewall,
16 assume to be a trusted relationship
17 because I am strongly authenticated, you
18 have got the same risks and
19 vulnerabilities that you have with the
20 VPN tunnel.
21 Whatever is on my laptop is on the
22 network and the fact that I am strongly
23 authenticated and I am just using it to
24 establish an uncontrolled unmonitored
25 path into the electronic security

1 perimeter I might as well just VPN
2 straight into the interior networks and
3 I have the same end result.
4 There needs to be something more
5 than just saying that we that a jump
6 host.
7 There has to be a functional
8 isolation between the remotely accessing
9 party and the target system.
10 I'm not going to mention technology
11 products, but there are definitely
12 products and probably most people are
13 aware of the types of products out there
14 that will provide that functional
15 separation and isolation.

MR. KINAS: There are tools out there that can help in that aspect.

Fortunately, we always try to step away from specific technology because the industry is changing and we all know that technology is changing faster than we can keep up with it.

However, when we put requirements in like the way they are now with Version 5, yes, Kevin has a good point

where the easiest solution is to RDP to your DMZ box and then you jump from there and do you just about anything you want.

So that it provides more than nothing, but does it provide enough? Probably not.

It is one of those where you have to do a lot more esoteric controls from a security perspective to monitor and manage that connectivity.

It is difficult to write those down in compliance requirement format.

We will probably need to do more, but I am not sure how it is we will get there.

MR. BOONE: From our perspective, it is a step moving forward, where an intermediary device does provide some

20 protection there and we are always going
21 looking to provide more with that
22 defense in depth here.
23 We need to set a threshold and
24 let's move forward and gain some
25 experience with it.

1 Just because it is a standard it
2 doesn't mean that that is where PHI
3 would stop. I mean we are certainly
4 always going to be looking at ways to
5 enhance our cyber security.
6 Standards are always going to
7 probably be lagging some behind. We are
8 doing some conversions to IP from serial
9 connection.
10 We are doing that because it is in
11 our business interest to enhance the
12 system. We don't necessarily need a
13 mandate.
14 I would agree with EEI. You have
15 to manage those risks, manage those
16 resources, and this does strike a
17 balance. It is a step in the right
18 direction and we should gain some
19 experience.
20 We indicated, if we run into
21 problems, we can have more technical
22 discussions and move forward.
23 DR. WRIGHT: Weak but light years
24 ahead of where we are on protecting the

serial SCADA commands that say open the

breaker.

Note that the remote access solution is using IP and IP technologies.

Clearly, we have decided that that makes sense economically and technically and we need to decide the same way for other parts of the system.

MR. GINTER: Waterfall is very concerned, as I said, about the risks of remote access of all sorts.

Interactive remote access is the attack method of choice, "the" attack method of choice, for advanced targeted attacks.

We believe that it is prudent, practical, and affordable to protect against these most advanced attacks and in the course of protecting against these most advanced attacks you, of course, have put measures in place to deal with the more mundane attacks.

This in my understanding. It is not widely understood in the bulk electric system.

I remember a meeting with a

prospective customer a number of months ago, we went through their needs, we went through offerings, and in the end the conclusion was, one of the people at the back of the room stood up, and said, "Great idea. Great technology. We are not going to deploy it. It doesn't fit our needs."

I am going, "Can you help me? Why?"

"It is because I don't like fighting traffic on Thursdays and Fridays, so I work from my basement on those days every Thursday and Friday."

I was dumbfounded, but in hindsight comments like the following spring to mind.

How many guards, gates, and guys with guns stand between the general public and the control system for your part of the power grid?

How many guys with guns and guards and gates hardwired stand between the general public and your basement or your

hotel room?

Why is it a good idea to control a large part of the bulk electric system from a hotel room?

I heard another speaker put it be a

little bit more bluntly where people were arguing that we need all of this interactive remote access no matter how risky it is.

The other speaker came back with, "If you have a compelling business need to control the bulk electric system from your cell phone while you are stopped at a traffic light over a VPN, we cannot help you, CIP cannot help you, nobody can help you. You are on your own."

Interactive remote access just strikes us as a very bad idea and is not nearly widely enough understood or thoroughly enough protected.

MR. BATZ: What we have in CIP Version 5 is a start, but it would be a mistake to believe that nobody anywhere will do one other thing other than what is in the standard.

On its face, I do not believe that that is the case. There are a number of tools that are available that are information sharing NERC alerts, guidelines that can be developed.

In fact, FERC itself has an Office of Energy Infrastructure Security that has been meeting with many utilities talking about best practices both related to physical security and cyber

security.

It is not correct to assume that as a general matter all entities will do only what they are compelled to do through mandatory standards.

That is not the case.

MR. PERRY: Respectfully, David and I have known each other for many years, and I have a lot respect for him, but I must respectfully disagree based on what I see at audit.

I have stated publicly and I am going to state it again. I would like the authority to write a violation for stupidity where an entity has a

corporate password policy that is stronger than the password policy for their CPI standards or for their CIP critical cyber assets because they did dumb down their policy to the minimum expected.

At audit my team does something that not all the regions do. We do as much outreach as we do auditing and it is one of the reasons why we do two weeks on site.

What we find is it doesn't matter whether you're a large investor owned utility or a small public power or a

rural electric entity, the guys who are down in the trenches desperately want to know how to do the right thing.

Management is getting better about letting us have those discussions now that they understand that we are not beating on their staff, but the guys in the trenches that need to do this desperately want to know how to do it.

That's the key message because the large investor owned utilities like

PEPCO, they have large staff and they can acquire the staff that has the expertise to do the very things that have been talked about.

But when you get out into such wonderful places as Anadarko, Oklahoma, Garden City, Kansas, Hayes, Kansas, Locust Grove, Oklahoma, it is very very difficult to even find experienced people who want to work in those lovely resorts spots much less being able to hire them and get them there.

What I am seeing is a lot of entities at least down in my region where the system administration is being done by electrical engineers who are very very good electrical engineers, but they are not cyber security experts.

They really don't know how to

approach what is required of them even in the existing more prescriptive standards. That gives me some concern there as well.

MR. DeFALAISE: I want to thank all the panelists for coming. Kevin Perry

has mentioned that there are two types of networks that we are third-party communication networks and then networks that are owned and municipally controlled by the entity outside of their ESPs.

Mr. Batz also alluded to that in looking at these networks or looking at the possibility of putting mandatory controls on those networks might be daunting because of limited resources.

We need to manage the risk and we don't have enough resources, so eliminate the risk, but we need to manage the best we can.

What NERC has done with CIP Version 5 and the industry coming back with the standard that was approved by the Commission, they took a new approach to this and they looked at from a risk standpoint, high, medium, low impact assets when applied to transmission like substations generation, could that same

technique be applied to these third-party -- I am sorry -- the

networks that are owned and administratively controlled by the entities, could we use that same approach with high-medium impact as we identified those networks that would allow us to apply some level of security but at the same time do it with the understanding of the limited amount of resources as Mr. Batz has alluded to?

With that, I will leave that to anyone to address.

MR. PERRY: Since how it is I broached the subject, I will start out.

The problem is with electronic security stuff travels at the speed of light and the weakest link is my attack point.

If I put my black hat on and I start thinking like an attacker, and I encourage entities that know their system very well, if I wanted to attack myself, how would I do it?

It is almost the inverse triangle. The little guy who cares about in terms of Big Iron is the weakest link.

If I can get a foothold in the network, I can go upstream through trusted communication paths.

ICCP, for example, I have to let the ICCP data traffic through my firewalls. I have no choice. It is part of my operating requirements.

TOP 5, RO-10 requires me to communicate with my RC and communicate with neighboring BAs and TOPs as necessary.

The little guy is just as critical as the big guy from a risk perspective when you're looking at interconnectivity of all of your control systems and commuter systems.

You cannot necessarily go, and say, "They don't have generation more than 1,500 megawatts. They do not have a substation with 3,000 points garnered because they have a bunch of big heavy duty lines coming in and out."

If you are a control center you are connected to other control centers then you need to be highly secured.

Period.

End of discussion.

I don't care if you are Pine Cone Power, as my friend Dave Norton likes to say, or you are the biggest electric

utility in North America, your control centers are equally vulnerable and I would even offer that the small guys are even more vulnerable.

Some of the other stuff, yes, maybe.

Like I said earlier, I am not advocating that you apply all the substandards, but there are some reasonable controls, some physical access controls, some electronic access controls.

I go out in the subs and the communication equipment is sitting inside the control house. There's access control on the control house, that is probably good enough.

When I go into the generating plants, maybe not quite as good when you have got a communications stack of

hardware sitting in an open rack in high traffic area, you can do better, you could put a cabinet around it with a locking door maybe.

Just to address some risk without having to spent a whole lot of bucks to do it.

You cannot put a huge dome around your Ethernet over SONIC network.

That's why I was advocating encryption between electronics security perimeters because it is all about the data.

I can put a lock on the door where my communications equipment is that outside of the ESP.

Today the CIP Standards don't require to you do anything and that's where the gap is. We need to do something and we don't need to break the bank to do it.

MR. PHILLIPS: Do you believe that we need to do anything as far as developing controls for components or data that is outside of the ESP or are the controls at the ESP right now

adequate?

MR. PERRY: Right now you have no controls for anything that is outside the ESP, so they're certainly not adequate. We need to decide what the security objective needs to be.

Do I protect the integrity and the availability of the data, and if so, what do I need to do to do that?

It is not just the CIP Standards.

COM1-1.1 today has language regarding high availability, divergent paths, redundancy, et cetera, and entities definitely recognize that wide

area network and entities are beginning to recognize that we are also talking local area network.

If it is critical communication, then you need to have no single point of failure from the source to the destination, obviously, the source computer, the destination computer are going to be single points, but you can team, you can do trunking, you can do divergent paths.

When I was managing the IT Department at Southwest Power Pool, I devised with one of our telecommunication guys what we call high availability ICCP.

It's multiple carriers. There is no single point of failure. It comes in different ends of the building, the equipment is at opposite ends of the data center, we have maximum separation of everything, to eliminate somebody stepping on a power cord and killing both ICCPs service.

It did not cost me anything to do that. I understand in COM1-2 that language has gone away and maybe there is a push to put it in the IRO-2 language.

19 If you've got reliability standards
20 that require you to have highly
21 available communication networks, then
22 you ought to have a requirement to
23 protect those networks to ensure the
24 high availability and then for the data
25 itself you need to do what you can to

1 assure the integrity and the
2 availability of the data because that is
3 what we are making decisions on and that
4 is what we are using to control and
5 without it we have got problems.
6 MR. PHILLIPS: With that in mind, I
7 would like to open this up to all the
8 panelists.
9 Do we need to develop a definition
10 in your view of communication networks
11 and would the definition change whether
12 we require physical controls or logical
13 controls?
14 MR. KINAS: To Kevin's point, the
15 infrastructure gets back to
16 availability.
17 Protecting those assets is one way
18 to attempt to increase availability to
19 make it harder for a hacker to
20 compromise those devices and interrupt
21 our communication.
22 There are other ways to do it.
23 If he said, "You can have multiple

24 communication paths. You can have them
25 diversely routed, that's another way to

1 enhance the availability aspect of it.
2 The communication networks
3 themselves we really need to focus on
4 the data that is traversing the
5 networks, that needs to be protected
6 which gets back to the objective-based
7 requirement.
8 It is unfortunate that we have been
9 hardware focused and we tend to get that
10 way.
11 As long as the objective is to
12 protect the confidentiality and the
13 integrity of the data entities should
14 have the choice to do by whatever means
15 they feel is the most appropriate.
16 It might be by implementing
17 hardware particular controls under
18 communications equipment.
19 It could be through other
20 cryptographic means at the source
21 devices or source servers.
22 They should have the freedom to
23 implement either one of those whatever
24 they feel is best.
25 Defining the specific term

"communication networks" kind of leans back towards the concept of physical protection, not providing the flexibility you should be allowed.

MR. BATZ: I appreciate the question. I would respectfully suggest that this is not the time for major shifts in requirements or standards.

It should be important to keep in mind that, frankly, it is in each utility's self interest to maintain effective communications structures for their base operations.

If need is not spinning and the bills are not going out the door, then there is a problem.

Sometimes it is challenging because people say, "The utilities should be compelled to do the right thing." Well, with all due respect, the very nature of the business kind of creates a stimulus for things like the availability of data networking in order to form baseline utility operations.

I recommend that near term like get

into the initial actual requirement dates of CIP Version 5 as it currently exists.

Let's work with the Commission,

with NERC, with the industry and the development of additional guidelines information.

Let us continue information exchange between industry and government to address emergent security risks.

MR. GINTER: It is a complicated question. Standard security practice says when you're moving information between security perimeters across a wide area network, yes, of course, it should be encrypted and to do that you need to define your terms and you need to put measures in place.

To me, the greater concern in a sense is a no brainer to me. The greater concern is when you have communications that are passing from a secure perimeter out into the world and terminating in end points that are not inside a controlled secured perimeter

such as a hotel room with interactive remote access.

The problem with all of the security mechanisms that are used widely for securing where I have a secured inside, and I don't know who I am talking to, the vast majority of these mechanisms are software based, and I'm sorry, but all software is vulnerable.

10 You may have discovered the

11 vulnerabilities and you may not have yet

12 discovered the vulnerabilities, somebody

13 else may have discovered the

14 vulnerabilities.

15 To me, when you have your highest

16 risks scenarios, when you are

17 communicating from a secure perimeter

18 out to who knows what, that's where you

19 need to look at your most effective

20 protections, and in my opinion, the most

21 effective protections for a security

22 perimeter are hardware based and not

23 software based.

24 MR. BARDEE: We thank the panel for

25 their remarks and the answers to the

1 questions. You have given us a lot to

2 think about and we do appreciate it.

3 Thank you all. We will take a 15

4 minute break and we will back at a

5 quarter of the hour.

6 (Panel 3)

7 2:45 - 4:15 p.m. NIST Frameworks Discussion

8 Patrick Miller, Managing Partner, The Anfield Group

9 Brent Castagnetto, Manager, Cyber Security Audits &

10 Investigations, WECC

11 Gerald Mannarino, Director, Computer System Engineering, New

12 York Power Authority

13 Melanie Seader, Senior Cyber & Infrastructure Security

14 Analyst, Edison Electric Institute

15 Jason Christopher, Technical Lead, Cyber Security

16 Capabilities & Risk Management, U.S. Department of Energy

17 * * * *

18 MR. BARDEE: Our speakers for the

19 third panel are now ready, so are we.

20 If we could have everyone take their

21 seats, please.

22 Our topic for the third panel is

23 essentially the NIST frameworks and how

24 they relate to the CIP Standards or do

25 not relate and whatever the overlaps are

1 and we have got five speakers on our

2 third panel for today.

3 I will start with Mr. Patrick

4 Miller and he is the managing partner of

5 the Anfield Group.

6 Mr. Miller.

7 MR. MILLER: Thank you, and good

8 afternoon. I would like to offer my

9 sincere thanks to the Commission for

10 holding the technical conference.

11 It is an honor to be part of this

12 esteemed panel and this is a very

13 important issue within the electric

14 subsector.

15 I am one of the few who have

16 drafted, implemented, audited, enforced

17 and advised on the NERC CIP standards.

I think I have been around the entire block on this one.

With that said, it is important to note critical infrastructure organizations have civic, fiscal, and moral duties to protect their systems from attack and they should be held accountable for these responsibilities.

However, adding overly prescriptive regulation may have the effect of introducing a competing prerogative, the fiduciary duty to avoid legal penalty for non-compliance.

This has the potential to divert resources from real, tangible security and reliability improvement efforts and there is a very real situation that we are creating where we fear the auditor more than the attacker.

But make no mistake though. The electric power industry is not waiting for regulation or new frameworks to secure their environments.

Successfully responding to and preparing for threats and risks and rapidly restoring the grid to a safe state of operation are industry-wide responsibilities and we take them very seriously.

Our utilities already respond to catastrophe with the skill and aplomb that only comes from years of experience and refined maturity.

They do this every day and they do it well.

Cyber security is another important variable in their risk landscape, but it doesn't significantly change the overall risk management approach.

Like all other risk mitigation efforts cyber security protections should support the mission of delivering safe reliable power to the consumer.

Legislation and regulation are certainly necessary to move us forward.

They form the structure and frame of reference for all of the various parties attempting to manage security risk for the industry.

I am in favor of certain types of regulation, however as a practitioner in this field, I caution that regulation can be a difficult vehicle with which to effect a net-positive change on security, cyber security in particular.

Many of the best-intended approaches are challenged to achieve their expected outcome.

The NIST cyber security framework has introduced a voluntary approach.

Note that many believe that this is only preliminary until it can gain enough acceptance and replace the existing regulations.

It is effectively seen as the de facto or quasi regulation already. It is discussed in expert forums as though it is regulation.

It is being requested through mandatory oversight venues such as State Public Utility Commissions and Regional Entities under NERC.

Whether voluntary or not the genie is out of the bottle.

While in favor of some regulation to establish minimum bars and guardrails I will always contend that hackers are faster than laws.

There is an existing body of legal precedent on the subject of cyber security and it has not stopped the flood of every increasing cyber security issues.

We have spent billions on required security and at some point we need to question whether our legislative

regulatory and enforcement structures are the only solution.

To be clear, I'm not implying that we should throw out regulation, rather we should look at places where regulation will work and where it won't.

Organizations should be fully aware of the vulnerabilities within their portion of the system. It is also important to know the threat actors, their motivations and activation triggers.

Additionally, it is important to know the potential impacts should a threat actor choose to exploit those vulnerabilities.

The CIP Version 5 Standard is effectively silent on the threat landscape and the security situational awareness portions.

It does speak to vulnerability management requiring utilities to manage

configuration baselines and track and evaluate and install patches for many systems or at least those that are updatable and where a patching source exists.

Impact is managed through methods of detection followed by incident

response and disaster recovery.

However these requirements vary as they are related to the high, medium and low impact categories. It is important to note that there are exclusions and allowances for lower risk and legacy systems which are often some of the weakest ones.

The risk management process and the cyber security framework both address threat, vulnerability, and impact arguably in greater detail than the NERC CIP standards.

In many cases they both account for the subtle differences between information technology and operational technology.

The NERC CIP Standards apply many

of the same methods to both with an allowance for technical infeasibility on legacy or ICS equipment is called out.

Everyone is left to choose their specific direction for their original CIP Version 1 risk based assessment methodology.

The degree of inconsistency was significant. I was as an auditor firsthand and I saw this as an utility trying to implement the original R-BAN.

The inconsistency ultimately led to

the creation of the bright line criteria within an Attachment 1 of CIP Version 4. It was an attempt to get a more consistent application of the process.

The bright line criteria does use an engineering-based approach leaning heavily on the NERC glossary of terms.which involves many engineering specifications but what happened was the CIP Version 5 model came thereafter and we ended up with a high medium low risk impact categories in addition to bright line criteria.

This added a lot of complexity to trying to determine what is in scope and how to apply the measures to what is in scope.

I would argue that none of the aforementioned approaches solved the problem.

When the binary critical approach was used in CIP Versions 1 through 4 many scrambled to exercise the flexibilities around routable protocols, engineering studies, etc, and we heard some of that in previous testimony.

They didn't do this intentionally to make their systems less reliable. They did it because of the cost

17 associated with being critical. That is
18 just an unfortunate reality and you
19 mentioned earlier about the unintended
20 consequences.
21 Now, in Version 5 a similar
22 approach is being taken around finding
23 the "right" position within the high,
24 medium, and low categories again costs
25 being a primary motivator.

1 In many cases it would have cost
2 the utility more to become compliant
3 than it would have them what they spent
4 in penalties for not being compliant.
5 Essentially you can prescribe
6 action but not attitude.
7 Early in the CIP Version 1
8 discussions an astute colleague of mine
9 with a long background in both
10 engineering and security has suggested
11 to come to the problem from a different
12 perspective.
13 His methodology for determining
14 criticality was very simple.
15 He stated: "If you would mind your
16 adversaries controlling that facility,
17 system, or cyber asset, then it's
18 probably worth protecting," Re: a binary
19 approach.
20 However, it simply isn't feasible
21 to protect everything to the same

22 degree. Some elements of the grid need
23 more protection than others.
24 Where we can't protect and prevent
25 or it may be unfeasible the most

1 effective proven options are detection
2 and response.
3 What isn't found in the CIP
4 Standards is the balance of detection
5 and response for the low impact
6 category.
7 Currently, we are trying to manage
8 risk through regulation and voluntary
9 incentive. In order for risk management
10 to be effective regardless of the
11 drivers we must understand the risks
12 enough to manage them.
13 Understanding requires analysis.
14 Analysis requires data and data
15 requires measurement.
16 We have very little cyber security
17 actuarial data in this sector.
18 Understanding that electric power
19 is without question the most critical of
20 the critical infrastructures it is easy
21 to fall into the trap that would say
22 that this type of information is just
23 too sensitive.
24 However, we've gathered sensitive
25 information data to improve and advance

healthcare, to enhance aviation, and automobile safety and even managed fraud in complex financial systems.

It can be done.

Without actuarial data from which to make informed and intelligent decisions we are essentially guessing and hoping we get it right.

Neither the CIP Standards nor the CSF or RNPs speak to mandatory or voluntary methods to obtain this actuarial data.

Whichever path we choose or which other path is chosen for us we should endeavor to maintain consistency.

Through consistency and measurement we will be able to determine whether or not we are actually making a difference.

Thank you.

MR. BARDEE: Thank you, Mr. Miller.

Nest we have Mr. Brent Castagnetto from WECC. He is the manager of Cyber Security Audits and Investigations for them.

MR. CASTAGNETTO: Good afternoon.

My name is Brent Castagnetto and I am the manager of Cyber Security Audits

Investigations, the Western Electricity Coordinating Council.

I appreciate the opportunity to discuss the NIST security risk management framework, the cyber security framework and the CIP Version 5 Standards.

The goal of my remarks is to highlight each and identify additional control objectives that may be considered in future revisions of the CIP Standards.

As has already been mentioned reliance on technology communication and the interconnectivity of information technology and industrial control systems has changed and expanded potential vulnerabilities and increase risk to the reliable operation of the bulk power system.

CPI Version 5, the NIST risk management framework, the NIST cyber security framework require

identification, categorization and protection of information systems and industrial control systems.

The NIST risk management framework leverages significant number of FISMA publications in the form of standards and guidelines that dictate its

8 overarching framework.

9 To ensure information systems meet

10 the minimum cyber security control

11 objectives identified in NIST's Special

12 Publication 800 Series.

13 The objective of the risk

14 management framework is to provide an

15 effective structure for selecting and

16 applying the appropriate security

17 controls for federal information

18 systems.

19 The NIST cyber security framework

20 builds on the concepts specified in NIST

21 800-53 and other 800 Series

22 documentations and uses components from

23 the control objectives for information

24 related technology.

25 The International Society of

1 Automation, or ISA, the International

2 Organization for Standardization and

3 International Electro Technical

4 Commission or ISOIEC, specifically the

5 27,001 Series.

6 The Framework core consists of five

7 aspects for current and continuous

8 functions to identify, protect, defect,

9 respond and recover.

10 When considered together these

11 functions provide a high level strategic

view of life cycle organizations management cyber security risk.

As directed by the Commission, the CIP Version 5 Standards Drafting Team worked to ensure CIP Version 5 Standards leverage the NIST risk management framework.

This is apparent from the CIP 2-5 identification and classification of BES cyber systems and through controls specified in CIP 5, CIP 7 and CIP 10.

The CIP Standards can be further strengthened through the application of additional control objectives listed in

these two frameworks.

For example, NIST special publication 800-53, contingency planning or CP-8, requires an organization to develop primary and alternate telecommunication service agreements that contain priority of service provisions.

This level of planning is not currently required by CIP 9-5 and would strengthen the registered entity's ability to remain connected ore reconnect its critical systems more rapidly when recovering from an incident or disaster.

NIST 800-53, physical and

environmental protection, specifically, PE-9 through PE-15 require an organization to ensure protection of power equipment and power cabling processes to ensure an orderly shutdown of information systems in the event of primary power loss.

Additional control objective is not currently found in CIP Version 5 or the

proposed physical security protection standard, CIP 14, include fire protection, temperature and humidity control and water damage protection.

Taking an all hazards approach these controls would strengthen a registered entity's ability to protect against and mitigate physical and environmental related vulnerabilities.

NIST statement 800-53, systems and communication protection, specifically SC-8 through SC-13, the NIST framework protection data security specifically PR.DS-6. Both require an organization to ensure data transmission, integrity, and confidentiality through the use of trusted communication paths, service certificates and cryptography.

Today's threats and vulnerabilities are more sophisticated and complex than

21 ever before and the use of malware
22 targeting data exfiltrations is growing
23 at an exponential rate which is one of
24 the greatest threats facing our
25 industry.

1 Leveraging these control objectives
2 may help ensure both data at rest and in
3 transit are managed in a secure manner.
4 The NIST cyber security framework,
5 specifically, protection protective
6 technology, PR.PT-4, require an
7 organization to ensure protections are
8 applied to communications and control
9 networks.
10 This may be considered by the
11 standard drafting team in its efforts to
12 address the Commission's remaining
13 concerns with Order 791.
14 The aforementioned control
15 objectives and protections are only
16 sample area that may be leveraged to
17 augment the CIP Version 5 Standards.
18 Cyber security control should be
19 based on risk and must be considered
20 with the security triad taken into
21 context and priority for our industry.
22 And that is availability, integrity
23 and confidentiality.
24 In summary there is no silver
25 bullet for the security of the bulk

power system.

Achieving long term security and reliability will require more than mandatory enforceable standards or voluntary frameworks.

The security to the bulk power system will require a more robust risk based approach.

We must approach security controls and frameworks as pieces of holistic solution applied in the manner commensurate to the risk profile of that which we are working to protect.

I would like to thank Commission staff for providing me the opportunity to share my perspective and look forward to meaningful dialogue and discussions as part of the panel.

Thank you.

MR. BARDEE: Thank you, Mr. Castagnetto. Next, we have Mr. Gerald Mannarino from the New York Power Authority.

MR. MANNARINO: I am Gerald Mannarino of the New York Power

Authority, director of Control Systems Engineering. Thank you for inviting me

to this panel.

The Power Authority has been subject to the NERC CIP Standards since December 2009.

Prior to the CIP Standards starting in 2003, we began our preparations for the voluntary Urgent Action 1200 Standard.

Under the current requirements we have identified our facilities, associated cyber systems, and physical security systems in order to implement and document the necessary controls.

We are now applying the CIP brightline criteria to assess and categorize our BES assets for Version 5.

In 2013, I attended the NIST cyber security framework workshops in order to participate in the development of the frameworks and learn how the frameworks could apply to the world of NERC CIP.

What I came away with was that the framework defines, as was its goal, a

broad-based adaptable model that can be used across the critical infrastructure sectors.

The framework core identifies a set of categories and subcategories of outcomes across five functional areas

which are identify, protect, detect, respond, and recover.

And the core then identifies informative references consisting of controls to address the outcomes.

Allowing for the goal of flexibility for the framework, the CIP Standards can be used as an informative reference.

We expect that industry trade groups will develop mappings of Version 5 to the framework to show that a strong alignment exists between them.

I believe the CIP Standards align well with the core as outcomes, rationale, and guidance as well as controls are described at length within the CIP Standards.

Using the NIST framework entities

would still use the CIP method for risk evaluation and identifying and categorizing assets for protection.

Both the NIST cyber security framework and the NIST risk management framework are open-ended regarding the asset identification and categorization process.

Terms such as business drivers and acceptance of risk are used.

These types of terms were present

in CIP Version 1 and were removed under FERC Order for Version 2.

Subsequent versions of the CIP standards have assumed a risk rating of one or zero, that is CCA or not a CCA, and no acceptance of risk or consideration for business drivers or business judgement was included in the standards.

As CIP has evolved Version 5 includes impact levels and risk levels similar to the frameworks and allows for more granularity in assigning controls at the high, medium and low levels.

A major difference between the CIP Standards and the two frameworks is the specificity of CIP to the BES assets and the supporting BES Cyber Systems, whereas the frameworks are general and meant to be used for any information system.

As a NERC reliability standard, it's appropriate for CIP to use facility ratings to identify the most critical BES systems and their cyber assets.

Enhancements to the brightline criteria could include additional support from system studies of the BES or from other NERC reliability

standards.

These studies could be expanded to test the impact of common mode failures that might be indicative of a cyber event.

The facility rating or the brightline method, however, potentially leaves out supporting cyber systems that may not have a direct or real-time impact on the BES assets.

The framework could help in this regard so that supporting systems outside the scope of CIP could be evaluated and appropriate controls applied.

Also, CIP doesn't account for external information services as was mentioned in the NIST risk management framework.

The cyber security framework presents a concept of establishing a profile that could represent the entity or even specific cyber systems.

The profile can be used to show current status as well as provide a target for a future state.

Similarly the profile could be used to establish a threshold for doing business with other business units within an organization or with external

organizations to the service providers.

This could drive vendors, consultants, and the supply chain to provide better products. It can also be used as a requirement for system to

system interfaces, interconnection agreements, and to address the "weakest link" concern.

Although the framework is only for critical infrastructure sectors would consult the vendors, consultants, and the supply chain to use it if the markets required it.

There are areas of the CIP Standards that are under modification as directed by Order 791 and we should see some clarification from the drafting team soon.

One issue that we see is the potential for scope creep as we identify and assess systems and facilities connecting medium impact sites and low impact and or out of the scope sites.

An area where security improvements can be made or in product development especially for control system devices authentication and authorization controls for field devices such as account and password management systems,

better inherent security features, and

device-to-device authentication would be welcomed improvements.

These improvements are outside the scope of the CIP Standards and the frameworks, however perhaps the NIST framework can be the market driver that addresses the improved products as part of a procurement language type concept.

In closing, I look at the CIP and the framework as having a complementary relationship.

The frameworks can form a picture and CIP fits into that picture and provides the focus for the BES which is really what we are trying to protect.

Thank you.

MR. BARDEE: Thank you, Mr. Mannarino. Next, we have Melanie Seader, senior cyber and infrastructures security analyst for the Edison Electric Institute.

MS. SEADER: Thank you.

Good afternoon members of the Commission Staff. I am Melanie Seader, the senior cyber and infrastructure

security analyst at the Edison Electric

Institute and I am here today representing EEI and our member companies.

We appreciate the Commission holding this conference.

The CIP Standards address cyber security to provide for reliable operation of the bulk-power system.

As the Commission stated in Order No. 791, CIP Version 5 is an improvement over the current Commission-approved CIP reliability standards that adopts new cyber security controls and extends the scope of the systems that are protected by the CIP reliability standards.

The low, medium, high impact categorization and the identify, assess, and correct language used in CIP Version 5 is based on the NIST risk management framework.

The NIST risk management framework is a methodology for implementing risk management activities into the system development life cycle of federal

information systems that support organizational mission and business processes.

In February 2014, NIST published the framework for improving critical infrastructure cyber security, the NIST

cyber security framework.

EEI and our member companies were engaged throughout the development of the framework and supported NIST's development of a flexible voluntary tool that leverages existing cyber security approaches.

Also through the Electric Subsector Coordinating Council we are now coordinating with the Department of Energy to develop sector specific guidance on implementing this framework which will include existing energy sector-specific standards used by the electric power industry, such as CIP Version 5 and the electricity subsector cyber security capability maturity model.

The NIST cyber security framework

provides organization and structure to today's multiple approaches to cyber security.

It is a voluntary risk-based framework to help critical infrastructure organizations to build a consistent and iterative approach to identifying, assessing, and managing cyber security risk.

In the cyber security framework,

NIST recognized that implementation is not a one-size-fits-all approach as risk is unique to the different sectors and organizations within each sector.

As a result, the tools and methods used to achieve the outcomes described by the framework will vary.

The use of the framework's cyber security activities are guided by an organization's risk management processes, legal and regulatory processes, business and mission objectives and organizational constraints.

This flexible approach enables

organizations to determine activities that are important to critical service delivery and prioritize investments to maximize the impact of each dollar spent.

These three approaches, the CIP Version 5, the NIST risk management framework, and the NIST cyber security framework all address cyber security, however each is very different and I will give you five examples.

First, CIP Version 5 is focused on the impact to the bulk power system reliability.

The NIST risk management framework

is focused on the impact to confidentiality, integrity, and availability of federal government information and information systems.

The NIST cyber security framework is focused on reducing cyber security risk to critical infrastructure, sixteen sectors with very diverse cyber security risk profiles.

Second, CIP Version 5 is mandatory

and enforceable for bulk power system owners and operators.

The NIST risk management framework is mandatory for federal agencies. The NIST cyber security framework is voluntary for critical infrastructure asset owners and operators.

Third, CIP Version 5 is compliance based requiring bulk power system asset owners and operators to document, report, and provide compliance evidence to external parties, in other words, NERC regional entities and FERC on specific security controls.

The NIST risk management framework is risk based giving federal agencies discretion in implementing security controls and accepting risk.

The NIST cyber security framework

is also risk based giving industry discretion or use of reasonable business judgment in implementing security controls and accepting risk.

Fourth, violations of CIP Version 5 result in financial penalties to bulk

power system owners and operators.

There are no financial penalties associated with the NIST frameworks which allow for internal auditing. Government audits government for the NIST risk management framework and industry audits industry for the NIST cyber security framework.

And fifth, because violations to CIP Version 5 results in financial penalties its language must be clear as to the implementation and compliance obligation it places on responsible entities and must not be too vague to audit and enforce.

The language of the NIST frameworks is flexible allowing its use or implementation to vary among federal agencies and critical infrastructure owners and operators.

CIP Version 5 will not guarantee security, but it will protect reliability of the bulk power system.

Voluntary standards and frameworks

such as the NIST frameworks allow

electric power companies to enhance their enterprise-wide cyber security posture which exceeds the scope of the systems that are protected by CIP Version 5.

The flexibility built into the NIST frameworks makes it difficult to incorporate risk-based concepts into the clear compliance language needed for the CIP Standards.

However much of the work already done to implement earlier versions of the CIP Standards will help electric power companies address core portions of the NIST cyber security framework.

The NIST cyber security framework can help electric power companies organize the various cyber security approaches used within a business unit or throughout an enterprise to identify opportunities for improvement which can be addressed using risk-based processes.

The extensibility of this approach enables companies to evolve their security practices in response to the

growing threat while remaining compliant

with local, state, and federal security mandates.

Another promising benefit of the NIST cyber security framework is its use as an internal and external communication tool to facilitate cyber security discussions among suppliers, management, government, and interdependent sectors.

However, when talking about the NIST cyber security framework and CIP Version 5 it is important to remember that both of these approaches to cyber security are new.

As the industry gains experience and reaches a steady state in implementing these new voluntary and mandatory approaches to cyber security we will be able to identify strengths and weaknesses based on implementation rather than theory.

This experience is essential to strengthening the voluntary and mandatory approaches we use to improve

the industry's security and resilience.

Thank you.

MR. BARDEE: Thank you, Ms. Seader. Finally, we have Jason Christopher from Columbus and also a technical lead of

cyber security capability and risk management for US Department of Energy.

Welcome back, Mr. Christopher.

MR. CHRISTOPHER: Good afternoon, Commission staff and fellow panelists. Thank you for the opportunity to join you today.

My name is Jason Christopher and I am the technical lead for cyber security capabilities and risk management in the Office of Electricity Delivery and Energy Reliability within the US Department of Energy.

Our office drives electric grid modernization and resiliency in the energy infrastructure through research, demonstration, partnerships, facilitation, modeling and analytics, and emergency preparedness and response.

We are also responsible for

executing the Department's role as the Federal government's energy sector-specific lead in responding to energy security emergencies both physical and cyber.

The department is not a regulatory body and as such does not implement or mandate standards.

Instead much of our work leverages technical staff's expertise in energy

systems operations and cyber security to establish effective relationships with the sector that results in more robust security bridging the well-recognized gap between security and compliance.

My comments today will focus on this relationship between mandatory cyber security regulations and various voluntary programs noting that there is no silver bullet as many have said today in any given cyber security standard.

The threat facing our nation's power grid is real and constantly evolving.

When attempting to address this

threat it is important that utilities leverage all of the tools at their disposal in addition to mandatory compliance programs.

Due to this relationship neither regulations nor voluntary guidelines can be developed in a silo as there may be compounding effects on industry when addressing various practices and requirements.

When the Commission released Order No. 706 in 2008, it directed the North American Electric Reliability Corporation to consider applicable

features of the National Institute of Standards of Technology's risk management framework when revising the CIP Version 1 Standards.

This NIST RMF refers to a six-step process for implementing and monitoring security controls and comprises of the Federal Information Processing Standards 199 and 200 as well as a collection of several NIST Special Publications.

The FIPS, which are mandatory for

federal agencies and federally-managed utilities enable organizations to apply various levels of security controls based on risk.

In essence, the standards require an entity to evaluate the impact due to a loss of confidentiality, integrity, or availability of data.

Security controls are applied based on a high, moderate, or low categorization resulting from this evaluation.

NIST publication 800-53 contains numerous controls logically grouped into eighteen security control families and cover technical, operational, and management requirements.

The publication is also accompanied with additional guidance for industrial

control systems like those used in power systems operations.

In September 2010, the Smart Grid Interoperability Panel Cyber Security Working Group co-chaired by the department released the NIST IR 7628

Guidelines for Smart Grid Cyber Security.

These guidelines, written by volunteers across federal, state, and local governments with asset owner operators, academia, and vendors, share many of the same concepts of the NIST RMF, but are tailored specifically for power systems operations.

Within guidelines for smart grid cyber security there is a similar discussion around high, moderate, and low impact categorization of data with the important distinction that power systems heavily rely on availability and integrity.

Furthermore, the guidelines apply these concepts independently to 22 logical interface categories or functions performed in power systems operations.

While smart grid is in the title of the document there are many routine

interfaces described such as the interface between transmission SCADA and

substation equipment.

The NIST IR describes amongst a variety of topics common technical controls as well as common controls for governance, risk, and compliance.

These requirements are applicable across all systems described in the guidelines document.

Additionally, each of the logical interface categories has their own tailored set of unique technical controls stressing the difference in operational requirements and associated risk for interdependent systems.

Two years later in May 2012, the department published both the cyber security capability maturity model, affectionately dubbed C2M2, and risk management process guidelines continuing the electricity subsector's public private partnership in developing voluntary cyber security guidelines.

Together, these programs help inform an energy company's cyber security program, allow for consistent

evaluation of their risk management efforts and help prioritize security investments.

The C2M2, which is accompanied by a self-evaluation toolkit consists of over three hundred practices in ten domains each of which were created by industry experts and piloted across 17 utilities before inclusion into the final document.

The model is not a collection of new practices. As a matter of fact, it leverages input from the NERC CIP reliability standards, NIST Special Publication 800-53, and the NIST IR 7628, among others.

The model's uniqueness is its assessment of the sophistication and management of a program's cyber security approach in accordance with maturity indicator levels.

A utility using the C2M2, based on their own risk profile can therefore measure improvements to their security program taking into consideration their

unique threats and organizational structure.

The electricity subsector risk management process guidelines co-sponsored by both NERC and NIST and

based on the NIST RMF, tailored risk management concepts from information technology with power systems operation technology practices.

The document outlines processes needed to frame, assess, monitor, and respond to cyber security risk across organizational boundaries within a utility.

Combined with the C2M2, the RMP provides guidance to a critical step in protecting an entity from cyber security threats.

This past February marked another important milestone in the public private partnerships focused on cyber security guidance.

As part of Executive Order 13636, NIST released Version 1.0 of its voluntary framework for improving

critical infrastructure cyber security.

The framework is the result of several workshops across the country, drawing inputs from various stakeholders across sixteen critical infrastructures including energy.

The framework is comprised of three elements, a core, tiers, and profiles.

The core which is a hierarchy of

cyber security activities grouped into functions contains several informative references including yet again NIST special publication 800-53.

These activities when combined with a risk management progression scale called Tiers help outline a current profile of an entity's security posture.

Within the life cycle of framework implementation an organization would also create a target profile based on future business needs and associated cyber security risks.

The department in collaboration with industry and interested government parties is in the process of writing

implementation guidance for the framework based on existing standards and guidelines including those mentioned today.

Since the approval of the CIP Version 1 reliability standards in 2008, the electricity subsector has participated in numerous voluntary cyber security efforts.

Historically, the industry has a strong track record of protecting our nation's power grid.

Cyber threats, however, continue to be dynamic and are becoming more

15 targeted and sophisticated.

16 The dynamic nature of cyber threats

17 underscore the importance of both

18 information sharing for awareness of

19 current threats and adoption of cyber

20 security standards and guidelines and

21 the need for an agile approach to

22 accommodate new threats.

23 In order to meet the risks

24 associated with these threats our public

25 and private partnerships will need to

1 continue to evolve.

2 This is an ongoing and complicated

3 endeavor. The department applauds all

4 the work of industry to date and looks

5 forward to continued collaboration in

6 improving our nation's security posture

7 across the energy sector.

8 While there are gaps between the

9 CIP Version 5 Standards and voluntary

10 guidelines there needs to be an

11 important dialogue regarding what

12 concepts are appropriate for inclusion

13 in mandatory regulations.

14 For example, the mapping submitted

15 to the Commission between CIP Version 5

16 and NIST IR 7628 shows gaps around

17 system acquisition.

18 While this is a point of concern in

industry there is also plenty of voluntary guidance around the topics including the department's release of the cyber security procurement language for energy delivery systems released just yesterday.

The concerns from FERC Order No.

791 regarding the security of communication networks supporting the bulk power system certainly need to be addressed as discussed earlier today.

The department continues its work with industry to identify actionable solutions for communications security in industrial control systems.

However, the department also recognizes the differences between mandatory compliance programs from many of the advanced best practices found in voluntary guidelines.

The department believes that advanced security controls should be applied according to a utility's own risk profile based on the evaluation of relevant threats, vulnerabilities, impacts, and likelihood.

While the CIP Version 5 Standards have taken an important leap in this direction by applying controls based on a high, medium, and low designations,

this appears to be based on physical impact of BES Cyber Systems according to

their voltage level and other power system characteristics.

As demonstrated in NIST IR 7628, it is possible to look at information flows and interfaces to evaluate what controls are necessary to protect power system functionality based on availability, integrity, and confidentiality of data.

The flow of data, and the appropriate interfaces would more accurately portray how a virus or malware would propagate through a utility which is important to consider when protecting assets and systems.

As future improvements of the CIP Standards are considered, this could be a potentially an important link in harmonizing traditional IT security with reliable operations of the bulk power system.

As the NERC CIP Version 5 reliability standards are implemented across industry there will undoubtedly be lessons learned.

There is no such thing as perfect

security. Security programs are more effective when measures implemented to achieve compliance are complimented with measures identified in voluntary guidelines that provide flexibility and may address more recent threats.

As utilities continue to improve their cyber security risk management programs, the relationship between mandatory compliance and voluntary guidelines will become more informed.

This process will not occur overnight, but will instead require diligence, collaboration, and persistence.

We as a sector should continue to work together to implement new standards, voluntary guidance, and programs to provide safe, reliable electricity to the American consumers.

I thank you for your time and look forward to a great discussion.

MR. BARDEE: Thank you, Mr. Christopher.

Mr. Miller, let me start with a

question for you. You raised a point in your statement that none of the other speakers today brought up.

I am referring to your suggestion

5 regarding actuarial data and setting
6 aside for the moment questions about how
7 that data might be gathered without
8 raising risks of it getting in the wrong
9 hands and just focusing on the issue of
10 what kinds of data you mean.
11 Could you say a little bit more
12 about what you have in mind there.
13 MR. MILLER: Right now we are
14 trying to measure whether or not we have
15 been effective with these standards.
16 That is the goal that I am trying to get
17 at, is that there are other models out
18 there that are similar in nature where
19 we have looked at mandatory approaches
20 and we have looked at how the regulatory
21 structures are designed and how do we
22 improve the regulatory oversight
23 functions and have the least amount of
24 unintended consequences.
25 One of the better models I have

1 seen that looks close enough to our
2 world is a lot like the FAA and how the
3 aviation system is managed for reporting
4 near misses and other operational
5 reliability issues and safety issues go
6 through a separate body and then there
7 are aggregates of that and then they
8 take a look at trends and make
9 regulations based on the outcome in

performance and trends.

It is in essence a way to get actuarial data in a safe way and there are existing models out there, but we can look at other structures too.

I don't want to overuse yet another analogy as the silver bullet and I don't have, "Here is exactly how you do it."

The point being is that we don't really have much in and we are guessing at this point.

We are trying to figure out if we are doing the right thing and in some cases we can say that we haven't had any cyber security related outages.

Are we sure? Do we have enough

measurement to say without a doubt, "That is true."

I don't think we do.

Until we can actually effectively get some solid detection, some solid measurements in there, it is hard for us to say that we really moved the needle.

That is my concern.

Does that answer the question?

MR. BARDEE: Yes, it does. But I will just give you a little more context for it.

Obviously, in other parts of what

my office is involved in we do have data like that, frequency responses, as an example, we get that kind of data all the time.

It comes in through NERC. People can quantify the impacts of events and judge whether we are that close or that close to a problem.

Again, setting aside the issues about the security of the data, there would be value if there were the right kind of data, but I am certainly not

expert enough to say what that data might be or how we would go about gathering it.

MR. MILLER: To give you another analogy. My background is actually field biology believe it or not, but when you study it, and it looks like in it is the book, and when you go out into the field and you realize that it looks nothing like it does in the book.

It is a complex arrangement of the surrounding events, all the other participants in the environment, its own genetics, there are many things that are at play.

In a situations where you don't have much to work with you just start measuring and then you base you science

19 even in some cases on bad measurements
20 but they are consistent enough to begin
21 building a foundation.
22 My point is that we need to at
23 least being to start measuring and to
24 start looking at options for
25 measurements where we could begin

1 generating trends and assumptions and
2 aggregate that data to make real and
3 appropriate decisions on whether or not
4 or improving our security posture, our
5 defense, and ultimately really our
6 resilience because we cannot prevent
7 everything.
8 MR. BARDEE: Mr. Christopher, you
9 mentioned in your testimony about the
10 guidance document that the department
11 issued yesterday and it actually came up
12 a little bit earlier in the day. I
13 don't know if you were here at that
14 time.
15 It talks about procurement concepts
16 and offers guidance on language that
17 could be useful and helpful in a
18 procurement arrangement in a contract to
19 ensure cyber security.
20 Could you tell us a little bit more
21 about the document since it just came
22 out yesterday?

MR. CHRISTOPHER: It is pretty much as you said mentioned it. It is procurement language for the purchase of

energy delivery systems.

It is just not electricity. It is also applying to oil and natural gas as well.

As I said with regards to my comments, when looking at how those may be applied for mandatory regulations, and why it was used as a specific example is because in the idea of system acquisition or procurement, this is beyond the technical discussion, I'm not a lawyer, so I can't really discuss that, yet I am married to one, which means I lose a lot of arguments.

With regard to the actual procurement language itself, you need to know who would then be liable in a supply chain risk.

That is where as Melanie's points were talking about, the difference in the CIP standards versus voluntary guidelines is with the penalties associated with them does the penalty for a supply chain go to then to utility, does it go further down the

road to the actual vendor and where does the authority begin and stop?

The procurement language has been a very powerful document. It has been great working with industry on that and seeing all the dialogue that has changed because of that, but it is also because it was in the environment of voluntary guidance to be able to be issued in the manner that it was.

MR. BARDEE: Putting aside for the moment the issue of whether something like that belongs in mandatory standards or not, just focusing on the issue as a potential vulnerability compared to other vulnerabilities in the cyber CIP context for electric utilities, what is your sense?

We have heard a lot about various exposures today, legacy equipment, worrying about compliance instead of reliability, you are familiar with a lot of those issues, how would you put this in context of that?

MR. CHRISTOPHER: One of the things

I think was really interesting, we did the whole framework process, so we are getting 16 sectors in the same room, or in many different rooms and we are

trying to discuss what security controls or practices should be applied across every one.

The interesting invalid that we had in that, and a lot of the industry members who were there would agree is we found out that because of some of these activities that we have already been doing, including compliance, we have been ahead of a lot of other sectors as a result.

There are some sectors that just don't have the robust dialogue.

For example, a lot of the dialogue that we have may be focused on business risks, whereas, some of the risks that we have today is based off criticality.

The risk discussion even across sectors has been very very different.

With regard to my own experiences having come from the regulatory space

into now a voluntarily program, I would say that there are no truths with regard to what a new witness where you may hear, "It is better to be at a large utility than a small utility."

That is not necessarily the case. It is really based off of the people who are there who are working on the ground

9 floor.

10 Some of these people in a small

11 utility may not have the bureaucracy

12 that they would have to get through to

13 get to get some certain protections done

14 quickly.

15 They can actually have a more

16 honest ally in some cases, whereas they

17 may not have the funding to be able to

18 do some new technical widget that would

19 be able to help improve security.

20 We focus now, for example, on the

21 C2M2 which is where I am drawing that

22 experience from on the processes and

23 what those look like for their own

24 security programs, not necessarily

25 focusing on the compliance programs.

1 You do see a little bit of a

2 disconnect between what the compliance

3 programs are doing with the security

4 programs are doing, but we are hitting

5 certain organizations a harmony between

6 those two.

7 MR. BARDEE: Do any of the other

8 speakers have something in that general

9 area? Mr. Miller?

10 MR. MILLER: I will add to that. I

11 can't say with the existing environment

12 that we are currently living with. In a

13 lot of cases the vulnerability is we are

tied to them based on their vendor relationships.

Net new going forward, having a stool touch as this very will be very transformational with respect to our ability to procure and insert the language that we need to at the outset, for example, in the RFP process, you don't even respond unless you can at least provide us some sensible answers to these questions that would essentially allows us to transform the

industry with our dollars which is really what is necessary at this point.

As long as we understand the demarkation between net new and legacy environments there is tremendous value going forward. I will echo that.

MS. SEADER: I can add regarding the procurement language document that just came out.

A big part of that was bringing vendors together along with electric power companies and other energy sector asset owners and operators, one of the challenges that they faced is the asset owners operators said would have varying requirements for cyber security.

Vendors would say, "You are the

only one asking for that." It is kind of both ways.

This effort was an opportunity to bring both the suppliers, city industry as well as industry together and agree on a baseline set of language and this language cannot be just dropped into a procurement. It is meant to just start

the discussion between the vendors and the assets owners and operators and it is really just to start at this point.

There will be further outreach going throughout DOE working with both communities.

MR. DeFALAISE: First question is for Mr. Christopher. In your travels to all the utilities that are using C2M2, are you finding that their entities that are also complying with the mandatory CIP requirements that are using C2M2, and if so, are they finding it, or are you experiencing it to be complimental environment where they are getting benefits from it? Can they exist together and do they help each other out?

MR. CHRISTOPHER: Let me start off with a rather large caveat which is with regard to the C2M2 program, we do not collect any data.

We do not share the names of any of the utilities that we have gone to, even to ones who have requested a

self-evaluation toolkit which is something that host internally at DOE.

With that being said, I can talk about anecdotals, but you will have take it for what it is, it is anecdotal.

To date we have given out the toolkit to, I want to say roughly to about 150 utilities in the United States.

In my conversation with utilities they have definitely had I would say interesting dialogues between what is going on in compliance and what is going on in security.

What we heard from the previous panel is that utilities are definitely resource constrained as they have to focus on compliance versus security and they have to make that decision and it is a very difficult decision to have to make and it does come back to that discussion of risk and what they view as being the larger risk, the risk of actually having an attack or the risk of an auditor coming in.

There should not be necessarily advocacy or a relationship between auditors and the actual security program.

In terms of whether or not these things can live together, they already do.

We do have a gigantic foreword in the beginning of the C2M2 that says, "that this does not bear any bearing whatsoever on your CIP compliance.

"If you have any CIP compliance discussion, you should go to your CIP compliance officer."

It is not meant to look specifically at the CIP Standards and that is designed on purpose.

It is supposed to be looking at the concerns that industry experts had that may in some cases go beyond the CIP Standards because the CIP Standards are looking at these baseline requirements.

The C2M2 is supposed to be able to provide road map from your current state to a new state and if it is only based

off of those baseline requirements and it is not going to be able to capture, "Where should I put my next dollar fro

my next investment?"

They do exist. They cohabitate the same space. They do compliment each in that respect.

MR. CASTAGNETTO: Anecdotally, from an auditor's perspective we have seen registered entities that have leveraged the C2M2 and they are very proud of it and then shared those lessons learned with us from an audit perspective to show how they have improved over time.

So we are seeing that. I would agree with you. We see that it co-exists.

MR. DeFALAISE: One last general question and this is for anyone.

We have talked a lot about these voluntary programs and all the benefits that are coming out of both with the supply change management with the new document that DOE produced yesterday, and also in with some of the earlier

panels we were talking about information sharing, that the information sharing, at least with the energy sector, or maybe in the Pacific fuel electric subsector seemed to gain traction and there is some kind of motion that would get some good work out that.

With that in mind, all of this

stuff is voluntary and FERC's main existence, if you would, it seems to be, at least for the effect of what we are here today talking about with the CIP Standards, mandatory, is there anything that FERC, from your opinions, is there anything that FERC could do to help out with what is going on or do you find that what is going currently right now with the industry and the government, DOE and DHS is moving along at a pretty good pace and doesn't need anymore assistance of anyone butting in on them, so to speak?

MR. CHRISTOPHER: I will go with that. DOE has had a very good relationship with FERC obviously and

most recently we are talking about framework limitations guidance.

We have representatives from both OER and OICE helping us out with that.

There is always an interesting conversation about how the dialogue may change when a regulator enters the room. We are talking about voluntary guidance, but I think that being able to have the technical expertise that FERC staff has on hand has been very valuable.

In the cases where the dialogue

would be further implemented by having that technical guidance and the technical help, DOE has already leveraged that and we continue to appreciate the help that FERC staff gives us on those matters.

MS. SEADER: In speaking about the implementation guidance for the frameworks.

On the industry side we come together through the ESCC, the Electricity Subset Coordinating Counsel we have developed a subteam to work with

DOE and then DOE coordinates with other federal agencies because it is not only FERC and DOE, but also NIST has an interest in it as well as DHS because of their CQ program.

On industry side we come together. We come up with up with comments and then submit that to DOE, so that kind of helps so we can freely share information among industry and then as a group we can come together and share that input.

That is very helpful.

MR. MANNARINO: I will chime in. One the earlier panelists mentioned about letting things settle.

We see a lot of organizations, the DOE, DHS, FERC, NERC, everyone has

different, whether different frameworks, different guidance documents, multiple versions of different frameworks.

It seems to be that we need to pick a direction, go there, and try to solve the problem with one thing.

There are too many meetings to go to solve all of these problems and they

are all converging on the same issues.

This framework workshop and that framework workshop, and this framework process, we need to settle somewhere.

MR. MILLER: From an information sharing standpoint there is a lot of different efforts because it seems every time I turn around there is another one that is forming.

There are a lot of folks who think that that is a bad thing. I disagree. I think it is a good thing.

If we look at the way we have been able to leverage technology to share information, at this point there has been actual scientific evidence that you will see the results of an earthquake faster through social media than you feel it travel through the planet.

That information sharing tool is profound.

Allowing information to be shared in ways that are useful and allowing the technologies and the natural social constructs around them is also very

useful.

There was a recent push around the target reach around getting a lot of the financial elements to begin to talk to each other because they were not.

This is different in other countries. We have our own approach here in the U.S., but in general allowing variations within information sharing structures and classifications and measures and means and technologies and layers, those can be very useful pieces.

People share information differently. Information is usually shared based on trust and trust usually requires relationships, and for us to share that without a preexisting relationship, we typically only share what we have to or what we are required to.

So be mindful around the requirements around sharing and those elements in order to allow this to happen naturally.

For example, inn the event of a real situation, a real active realized threat having that go through one specific point can be useful but allowing for alternate measures for neighboring utilities, for example, may also be useful.

MR. CASTAGNETTO: Along those same lines, it will take three part communication and we would have to invite you, but from a regional perspective we would love to see more participation at our various outreach functions to Patrick's point about building relationships from the pool within the industry where we see a lot of FERC staff during audits and in audit engagements and they can interact there, but I think reaching a broader audience to bring your technical expertise to bear would certainly help from a regional perspective and build relationships and establish that trust level.

MR. PHILLIPS: Understanding the

sensitivities around getting to a steady state, I will pose these questions in the far distant future context.

Could the panelists speak to any additional attributes that should be considered in the future when dealing with categorization of those assets for the high, medium, and low categorization?

MR. CHRISTOPHER: I will just repeat pretty much what I said in my opening remarks.

We have done this exercise a few times where we have looked at tailoring traditional IT practices towards what goes on in operational power systems.

Caveating with the multiple caveats in the galaxy future in the future and the fact there needs to be a steady state, looking at that harmonization and particularly looking at the categorization according to data flow.

This was actually mentioned on the previous panel as well but I am not sure if it was really picked up on, but the

fact is when we are talking about protecting information there is a reason you are protecting that information and that will be based off the impact, the availability, the integrity, and confidentiality of that data.

We have as a sector done that

before. There could be some more information gleaned from that and that is also to somewhat echo what Patrick said earlier with regard to data analytics.

The fact to be able to do that you will need to do a lot more data analytics where you have to actually know why you would be protecting certain systems and interfaces the way that you would.

An example here to compliment Patrick's earlier comment is if the Commission were to ever get based off of a sharing service, right, so if you had an actual sharing service agreement, there would be a lot of studies to back up why it is that that would be either

the largest contingency or a subsection of that largest contingency so a smaller megawatt value.

To be able to see some actual hard science behind some of these things would be in my opinion as a shared security researcher would be a very interesting discussion.

MR. BARDEE: Let me follow up on that. I am sure most of the people here and certainly the people on that side of the table know a lot more about this

13 topic than I do.

14 One way to look at the CIP

15 Standards is to say let's focus on the

16 big power facilities, the control

17 centers, the bit generation facilities,

18 et cetera, and look from there out and

19 see how could anyone get to my big

20 assets?

21 How could they get in?

22 I look at the NIST approach of

23 confidentiality, integrity,

24 availability, and to me it is almost

25 like looking from the other side of the

1 spectrum and saying, "I am on the

2 outside. How am I going to get in to

3 all of these facilities?

4 It is not clear that you

5 necessarily get a different result. It

6 is just starting from a different point

7 on the spectrum.

8 MR. CHRISTOPHER: A part of that

9 perspective of that is because the CIP

10 Standards are bound to the Federal Power

11 Act 215, which as you look at reliable

12 operation as the impact.

13 It is not to say that what we

14 already have in the NERC Version 5

15 Standards today is inaccurate to look at

16 impact, but impact is one part of the

equation when adjusting risk.

Risk does look more at the threats and the vulnerabilities that is inclusive of the impact and the likelihood as well.

If you're going to be looking at the protection of information it would be impact, certainly, and that is a great scoping mechanism as it is a very

important scoping mechanism for CIP.

But there is more when you are discussing data and when we are discussing the actual use of that data and having not what that data would look like, with what having a false data would look like, or having insecure data look like in terms of confidentiality.

Having that more robusted discussion would be really great.

That being said, it has happened like I said in NIST IR 628 it has actually happened in CIP Guidance too.

It is not like the sectors do not have this discussion. It is just a matter about where is it in terms of the availability today.

MR. MILLER: I have a lot of really good friends who are engineers and I have grown up in the power industry.

There is a lot of engineering

22 focused on the existing brightline
23 criteria and there is a lot of really
24 good value for that.
25 But there is a difference when you

1 are looking at this from a security
2 perspective.
3 Engineering really deals with
4 physics. Engineering deals with Mother
5 Nature.
6 Mother Nature may be harsh, but she
7 is not malicious. Your intelligent
8 adversaries are.
9 In a lot of cases, for example, 15
10 minutes from an attacker's perspective,
11 I can drop a lot of payload inside of 15
12 minutes and there can be a lot of damage
13 done within 15 minutes and in some cases
14 it will not manifest itself into an
15 outage. It may only be controlled.
16 Loss of integrity of the operating
17 environment whether there is an outage
18 or not is still a concern.
19 It doesn't speak to that. Those
20 are some areas that we still have some
21 gaps.
22 If I had my druthers I would say
23 that we at least take a look at this
24 with both lenses of engineering and
25 security and somehow find a median in

between where we can balance the approach.

It is not going to be an easy discussion. There will be a lot of turf wars and some arrows in the mix, but we still have to have this healthy dialogue around balancing the differences between the engineering aspects and the security aspects.

Because, frankly, as it is compromise does not always mean outage. There are some key pieces that we are frankly just overlooking from the overall threat of vulnerability and impact landscape.

MR. BARDEE: We wish to thank all of the panelists for being here today.

We appreciate your comments, and as I mentioned at the start of the day we will be putting out a notice setting a deadline for anyone who would like to submit comments in writing on the topics discussed today or listed on the agenda for today.

That will come out later this week

and we look forward to receiving those comments and considering them.

Thank you all.

UNITED STATES OF AMERICA)
ss:
DISTRICT OF COLUMBIA)

I, T. S. HUBBARD, JR., a Notary Public within and for the District of Columbia do hereby certify that the witness whose deposition is hereinbefore set forth was duly sworn and that the

11 within transcript is a true record of the testimony

12 given by such witness.

13 I further certify that I am not related

14 to any of the parties to this action by blood or

15 marriage and that I am in no way interested in the

16 outcome of this matter.

17 IN WITNESS WHEREOF, I have hereunto set

18 my hand this 6th day of May 2014.

19 _____
Thomas S. Hubbard, Jr.
20 Notary Public District of Columbia
Commission Identification 237435
21 Sworn in on June 12, 2006
Commission Expires April 30, 2018
22

23

24

25