

THE PUBLIC SERVICE COMMISSION OF SOUTH CAROLINA
COLUMBIA, SOUTH CAROLINA

PROCEEDING #14-11455

DECEMBER 17, 2014

2:45 P.M.

ALLOWABLE EX PARTE BRIEFING [ND-2014-38-E]

REQUESTED BY DUKE ENERGY CAROLINAS, LLC (DEC) AND DUKE ENERGY PROGRESS,
INC. (DEP) – CYBERSECURITY

TRANSCRIPT
OF
ALLOWABLE EX PARTE BRIEFING

COMMISSION MEMBERS PRESENT: Nikiya M. 'Nikki' HALL,
Chairman; Swain E. WHITFIELD, *Vice Chairman*; and
COMMISSIONERS John E. 'Butch' HOWARD, Elliott F. ELAM, JR.,
Comer H. 'Randy' RANDALL, Elizabeth B. 'Lib' FLEMING, and
G. O'Neal HAMILTON,

ADVISOR TO COMMISSION: Joseph Melchers, General Counsel

STAFF PRESENT: B. Randall Dong, Esq., Josh Minges, Esq., and David
Stark, Esq., Legal Staff; Philip Riley and Doug Pratt, Advisory Staff;
Jo Elizabeth M. Wheat, CVR-CM/M|GNSC, Court Reporter; and William O.
Richardson and Deborah Easterling, Hearing Room Assistants

APPEARANCES:

*FRANK R. ELLERBE, III, ESQUIRE, and ALEX CASTLE,
ESQUIRE,* along with *DARREN MYERS* [Managing Director of
Enterprise Protective Services / Duke Energy] and *HAFID
ELABDELLAOUI* [Managing Director of IT Security & Compliance /
Duke Energy], presenters, representing DUKE ENERGY CAROLINAS, LLC,
and DUKE ENERGY PROGRESS, INC.

*C. DUKES SCOTT, ESQUIRE, and ANDREW M. BATEMAN,
ESQUIRE,* representing the SOUTH CAROLINA OFFICE OF REGULATORY STAFF

PUBLIC SERVICE COMMISSION OF SOUTH CAROLINA

101 EXECUTIVE CENTER DRIVE
COLUMBIA, SC 29210

POST OFFICE BOX 11649
COLUMBIA, SC 29211

WWW.PSC.SC.GOV

I N D E X

	<u>PAGE</u>
<u>OPENING MATTERS</u>	3
<u>MR. ELLERBE</u>	3
<u>MR. CASTLE</u>	5
 <u>PRESENTATION</u>	
<i>MR. DARREN MYERS [DUKE ENERGY]</i>	7
<i>MR. HAFID ELABDELLAOUI [DUKE ENERGY]</i>	15
Question(s)/Comment by Commissioner Hamilton.....	25
Question(s)/Comment by Commissioner Randall.....	28
Question(s)/Comment by Commissioner Fleming.....	30
Question(s)/Comment by Commissioner Howard.....	33
Question(s)/Comment by Commissioner Fleming.....	35
Question(s)/Comment by Vice Chairman Whitfield.....	36
Question(s)/Comment by Commissioner Elam.....	39
Question(s)/Comment by Mr. Melchers.....	41
<u>REPORTER'S CERTIFICATE</u>	44

Please note the following inclusions/attachments to the record:

- *Physical Security Update* PowerPoint presentation slides (PDF)
- *Cyber Security Update* PowerPoint presentation slides (PDF)

For identification of any additional referenced materials, please see ORS correspondence filed as part of the *ex parte* briefing process.

P R O C E E D I N G S

1
2 **CHAIRMAN HALL:** We'll call this hearing to
3 order and ask our attorney, Mr. Melchers, to please
4 read the docket.

5 **MR. MELCHERS:** Thank you, Madam Chairman,
6 Commissioners. We are here pursuant to a request
7 from Duke Energy Carolinas, LLC, and Duke Energy
8 Progress, Inc., a request for an allowable *ex parte*
9 communication briefing scheduled for today,
10 December 17th, in the Commission hearing room at
11 approximately 2:30, and the subject matter to be
12 discussed at our briefing is: Cybersecurity.

13 Thank you, Madam Chairman.

14 **CHAIRMAN HALL:** Thank you.

15 Mr. Ellerbe? You want to introduce your --

16 **MR. ELLERBE:** Frank Ellerbe here for the
17 companies, DEC and DEP. And Madam Chairman and
18 members of the Commission, I'm going to talk about
19 a procedural issue that's presented by this
20 briefing, and then I'll turn it over to Mr. Castle
21 to introduce the presenters.

22 And the thing that I wanted to touch on
23 briefly is -- and we've talked to our presenters
24 about it -- the subject matters, the physical
25 security and cybersecurity of the systems, are a

1 matter of great concern; of course, that's why
2 we're making a presentation to you about it. The
3 thing that I wanted to bring to your attention is:
4 The provision of our *ex parte* briefing statute,
5 which is, as y'all know, 58-3-260(A) -- excuse me
6 -- (B)(6)(a) requires that anytime someone giving a
7 briefing talks about a document or passes it out or
8 refers to a document, then that document has to be
9 made a part of the record, which then makes it
10 available to the public in general.

11 So what we've asked the presenters to do is to
12 be very careful, because they know about some
13 documents that are very confidential, and we would
14 -- none of us would want those documents to be
15 available on the Internet. And so we are hoping
16 very much that this presentation will proceed and
17 we'll get finished without any reference being made
18 to such a document.

19 And the main reason I'm standing up here is so
20 y'all will be aware that we've asked these
21 gentlemen to do that and to be very careful. So if
22 y'all ask a question, you may not have in mind
23 asking about a document, but it may call upon them
24 or cause them to think that they would refer to a
25 document, but we've asked them not to do that. And

1 so we're hoping to -- again, by talking about it at
2 the front end -- avoid any issue with it.

3 So, with that being said, I'm going to turn
4 things over to Alex Castle.

5 **CHAIRMAN HALL:** Thank you, Mr. Ellerbe.

6 **MR. CASTLE:** Good afternoon, Madam Chair and
7 members of the Commission. I haven't appeared
8 before you in a while, so it's good to see you all
9 again. I am here substituting for Heather Smith,
10 who unfortunately was unable to be here because of
11 some illness issues. She sends her regards and her
12 apologies for being unable to come today.

13 But as Frank alluded to, this is a very
14 important topic and it's a very timely one for us
15 as a company, as we're continuing to take a number
16 of measures to protect company assets and our
17 customers' data and our own data from cybersecurity
18 and physical security threats that seem to be
19 increasing over time.

20 We have two very well qualified folks from the
21 company to come speak to you today. First I'll
22 introduce to you -- his presentation is up on the
23 board; his name is Darren Myers, and he is the
24 managing director of Enterprise Protective Services
25 for Duke Energy. He's been in this role since May

1 2013 and, otherwise, has six years of experience
2 with Duke Energy. He's currently responsible for
3 Infrastructure Protection Services, Operational
4 Security, Preparedness Services, and Security Risk
5 & Compliance. And, importantly, he has well over
6 20 years of experience in the security field,
7 serving in various industries, including the energy
8 sector. Also, importantly, Darren serves as an
9 alternative voting member at the NERC on the
10 Critical Infrastructure Protection Committee where
11 he's the chairperson of the NERC Business
12 Continuity Guideline Task Force.

13 Appearing today with Darren is Hafid
14 Elabdellaoui. He is the managing director of IT
15 Security & Compliance for Duke Energy, a position
16 that he has held just for the last three or four
17 months here at Duke. Within that role, he's
18 responsible for Access Services administration,
19 Security Architecture, Cybersecurity Operations,
20 and IT Compliance. Hafid has been with Duke for
21 over 12 years with various roles within the IT
22 Security & System Architecture groups within the
23 company.

24 So, with that, I will turn it over to Darren
25 so he can begin his presentation.

1 **CHAIRMAN HALL:** All right. Thank you. We're
2 glad to have you both, Mr. Myers and Mr.
3 Elabdellaoui.

4 Before we begin, I just forgot to mention and
5 recognize Andrew Bateman here, representing ORS.
6 So thank you for being here today, Mr. Bateman.

7 All right, Mr. Myers. It is all yours. Thank
8 you.

9 [Reference *Physical Security Update* Slide 1]

10 **MR. DARREN MYERS [DUKE ENERGY]:** Thank you for
11 the opportunity to come present to you today. So,
12 I'm going to be talking about our Physical Security
13 Program and as it relates to recently approved FERC
14 Standard -- or, NERC Standard cross-functionality.

15 [Reference *Physical Security Update* Slide 2]

16 Duke Energy has over 3200 substations across
17 our footprint, and they're all very important to
18 us.

19 The historical approach to security at those
20 assets was typically focused on premise liability
21 issues. So, it's fencing, signage, locks, keys,
22 access control.

23 [Reference *Physical Security Update* Slide 3]

24 In 2013, as a result of a sabotage event at
25 Pacific Gas & Electric -- referred to as the

1 Metcalf Substation -- there's been a shift in the
2 industry to implement physical security standards.
3 So, in February of this year, there was an order
4 that directed NERC to work very quickly to develop
5 standards to submit back to FERC. Those were just
6 approved in November.

7 So, with Metcalf, there were over 100 shots
8 fired into equipment at the substation that served
9 the Bay Area, Silicon Valley. There were some
10 telecom lines that were severed in a vault across
11 the highway behind the set of railroad tracks
12 underground.

13 And, despite that, there were no outages, and
14 it really didn't get a lot of attention at the
15 time, because it was the morning following the
16 Boston bombing, and so media attention was
17 basically focused there. There were some
18 congressional inquiries behind the scenes, but
19 then, in February of this year, the former FERC
20 chair went public on the front page of the *Wall*
21 *Street Journal* and talked about the vulnerability
22 of the grid, which there were no outages as a
23 result of Metcalf because of their ability to work
24 around the situation, using their resiliency plans.

25 But that shift ended up causing NERC to draft

1 a standard that has six elements in it. The first
2 three are related to identifying assets that could
3 have potential impacts to the bulk electric system
4 in the context of cascading outages and
5 instability, and the last three components of the
6 standard are around physical security, and one is
7 to have a security vulnerability assessment
8 methodology; one is to do assessments and identify
9 vulnerabilities and create a plan; and the third
10 requirement requires a third party to validate that
11 the methodology that was developed is appropriate,
12 that it was applied correctly, and that the plan
13 sufficiently addressed the vulnerabilities that
14 were identified during the assessment.

15 [Reference *Physical Security Update* Slide 4]

16 So, the Duke Energy approach to this was to
17 organize a Transmission Security Program, and there
18 are a number of work streams involved in that, and
19 it's a relatively new program because of the
20 newness of the standard. And there's not been a
21 lot of work done yet; we are just now starting to
22 move forward with the electric system analysis, and
23 that modeling will determine what assets are in-
24 scope of the new CIP standard, and we really don't
25 know what that list looks like today. We think

1 it's relatively small across the entire service
2 territory, but they have to finish doing the
3 modeling and, much like the security vulnerability
4 assessment, there also has to be a third-party
5 validation of the methodology that the Transmission
6 Department uses to do the analysis. So it gets
7 checked twice.

8 When the list is complete -- and there is a
9 timeline attached to the last page; it essentially
10 states that, throughout the course of 2015, we have
11 to complete the assessment and have the validation
12 done in the October timeframe, and then subsequent
13 to that we'll be on target to start implementing
14 plans. Well, because these assets are so important
15 to us and reliability is so ingrained in our
16 business, we did not delay in beginning the
17 assessments. So, based off of a preliminary
18 assessment, we came up with a relatively small list
19 of assets and we've engaged a third party to go out
20 and look at those -- the measures that are in place
21 -- with us. And that qualifies, according to the
22 requirements of the standard, and we are waiting
23 for some draft reports from that organization.

24 So, the work streams, in addition to the
25 electric system analysis and the security analysis,

1 also include expanding our capability as it relates
2 to monitoring threat information. So there's a lot
3 of cybersecurity threat information that Hafid will
4 talk about. This has caused an increase in media
5 attention to physical security issues, so we're
6 starting to see more of that. But, overall,
7 there's a lack of available information across the
8 industry and information sharing that helps us to
9 prepare, and perhaps it is that the threat is
10 really negligible; but as a part of our cross-
11 functional team, we're working on developing a
12 platform that will allow us to receive information
13 from law enforcement partners, from other external
14 industry sources, and cross-functionally between IT
15 Security and our Operations Department, so that we
16 all have the same view of the threat landscape.

17 Then, as part of this effort, we've also had a
18 lot of industry engagement with the Electric Power
19 Research Institute who has stood up a project to
20 look at specific measures that could be implemented
21 to harden assets that are determined to be critical
22 to the bulk electric system, and then we're also
23 working with the North America Transmission Forum
24 to work on some processes that will ensure that the
25 electric system analysis is being viewed

1 consistently across the industry -- because even
2 though we develop a methodology and we apply that
3 and we have a third-party review, other entities
4 could potentially do the same analysis and, if they
5 don't use the third party, then there could be a
6 potential gap. So working through the Transmission
7 Forum, they're trying to put some criteria around
8 that analysis, and that will help give us a better
9 view cross-functionally across the industry.

10 Then we also have a Solutions & Standards
11 group, which is really just part of our Engineering
12 Department. And if we determine that we have
13 assets that are in-scope of cross-functionality,
14 and we do vulnerability assessments and determine
15 that we have to put protective measures in place,
16 that group will help us to develop a standard so
17 that we can apply those measures consistently.

18 [Reference *Physical Security Update* Slide 5]

19 So, the next slide is really the details of
20 the requirements that I talked about in the CIP-014
21 standard. It's the electrical system analysis, the
22 verification, and a notification to the
23 transmission operator for the region that has
24 control that there are assets in-scope, and then
25 the security assessment, documented physical

1 security plan, and a third-party review. And a
2 timeline is attached at the end.

3 [Reference *Physical Security Update* Slide 6]

4 Let's see. The applicability -- so, what's
5 in-scope of the standard, we start out with a much
6 smaller set of stations than our entire inventory.

7 We're looking at modeling for: 500 kV or
8 greater; facilities operating between 200 kV and
9 499 where it's connected at 200 kV or higher to
10 three or more nodes, or modules; and then stations
11 that are identified by the reliability coordinator,
12 planning coordinator, or transmission planner as
13 critical would also be in-scope. Additional
14 considerations are stations that are essential to
15 nuclear plant interface requirements and control
16 centers.

17 [Reference *Physical Security Update* Slide 7]

18 And the last slide is the timeline that lays
19 out requirements to meet the electric system
20 analysis and development of plans, and a third-
21 party analysis, and then the implementation
22 activities occur after that December 2016 date
23 that's listed.

24 Because these stations are so important to us,
25 Duke Energy is also undertaking a project to

1 develop some methodology to tier assets for local
2 system criticality and also a business-significant
3 category that would allow us to have some standards
4 around applying security measures because the
5 assets are important to a significant event, such
6 as the Democratic convention or the Republican
7 convention, or it could be anything that's declared
8 by the Department of Homeland Security as a
9 national security event. We also want to make sure
10 that, where we have recidivism -- you know, repeat
11 instances of criminal activity and unauthorized
12 access -- that we're taking appropriate measures to
13 ensure that we keep people out for, you know, first
14 and foremost, public safety, but also for
15 reliability, and then it will help minimize our
16 losses related to copper theft and vandalism.

17 So, one phase of the Transmission Security
18 Program that I discussed that is in its infancy is
19 to focus on compliance with the NERC CIP-014
20 standard, but then part of our strategy is to also
21 go above and beyond for a limited number of assets
22 that would be very important for reliability at a
23 regional level or because they are important to
24 other critical infrastructure events or because
25 we've had repeat incidences.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

Do you have any questions for me?

CHAIRMAN HALL: I think we'll hear from Mr. Elabdellaoui before we go to questions. Okay? Thank you.

[Reference *Cyber Security Update* Slide 1]

MR. HAFID ELABDELLAOUI [DUKE ENERGY]: First of all, again, thank you for having us this afternoon to talk to you about --

CHAIRMAN HALL: Mr. -- yeah, when the red is on, and if you'll pull it a little closer to you, please.

MR. HAFID ELABDELLAOUI [DUKE ENERGY]: Okay [indicating]. Is that better?

CHAIRMAN HALL: Uh-huh. Thank you.

MR. HAFID ELABDELLAOUI [DUKE ENERGY]: Again, thank you for having us over, to speak with you about cybersecurity in general and talk to you about the steps that Duke Energy is taking to protect its cyberassets.

I brought some reinforcements with me, just in case there are questions that I'm not able to answer, who are three key leaders from our Cybersecurity Program: Carl Cahill is responsible for the security architecture of our systems.

MR. CARL CAHILL [DUKE ENERGY]: [Indicating.]

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

MR. HAFID ELABDELLAOUI [DUKE ENERGY]: Paula Guginò is responsible for our IT Security & Compliance Program.

MS. PAULA GUGINO [DUKE ENERGY]: [Indicating.]

MR. HAFID ELABDELLAOUI [DUKE ENERGY]: And Jeremy Carswell is responsible for the Cybersecurity Operations Program.

MR. JEREMY CARSWELL [DUKE ENERGY]:
[Indicating.]

MR. HAFID ELABDELLAOUI [DUKE ENERGY]: No doubt that lately you've seen increased coverage of cybersecurity events, whether it's on a newspaper or it's on television. So, in our discussion today, I will briefly cover some of the events that have occurred over the past 12-13 months in the industry, and spend some time with you to speak to you about what are some of the threats that we see and risks related to Duke Energy, specifically, and what are we, as a company, doing to address those or mitigate those risks. So, hopefully, by the end of this presentation, I'd like for you to walk away with the fact that, you know, while the number of cyber events are increasing in number, sophistication, as well as impact, that we at Duke Energy recognize that and we are working tirelessly

1 to ensure that our defenses are continuously
2 improved and we are taking all the steps necessary
3 to make sure we protect our assets.

4 [Reference *Cyber Security Update* Slide 2]

5 So, in front of us are some of the major
6 breaches that have occurred over the past 11 years.
7 And you'll notice, from 2003 to 2010, we
8 experienced a small number of cyberevents; that's
9 as it relates to breaches and impacts to companies
10 like TJ Maxx. And from 2010 to 2014, in the span
11 of four years, the number of cyberevents and
12 cyberbreaches has increased dramatically. No
13 doubt, you've seen in the news that Target was
14 impacted about 13 months ago, the likes of Home
15 Depot, JP Morgan, and, as of late, Sony.

16 Just to hit on some of the things that have
17 been going on over the past 12-13 months, Target
18 was breached and a malware by the name of BlackPOS
19 was installed on their POS systems and the bad guys
20 were able to walk away with over 40 million
21 records. A different strain of the same malware
22 was used at Home Depot and, again, the bad guys
23 were able to walk away with over 15 million credit
24 cards. JP Morgan, it took a single e-mail that was
25 clicked on by a web developer -- it was a phishing

1 e-mail -- and that gave the bad guys a way inside
2 the network. After they were breached, there was a
3 loss of about 80 million records.

4 So, at the end of the day, we are seeing that
5 the sophistication level of the cyberattacks and
6 the cyberbreaches are increasing daily.

7 In 2014, we also experienced some major
8 vulnerabilities. I will explain a vulnerability
9 called Bash: While the vulnerability is not new --
10 it really existed for 22 years -- it was
11 highlighted during this year in that it was a
12 vulnerability that could potentially provide a bad
13 guy the ability to execute code remotely on an
14 asset over our network -- or any network, for that
15 matter. While we at Duke Energy really did not see
16 any events related to Bash, we had to work -- we
17 had to spend a lot of time and a lot of hours and a
18 lot of money -- to make sure that we are addressing
19 this vulnerability and that we are patching our
20 systems, we're putting the right signatures, if you
21 will, on our perimeter, as well as in our network
22 to ensure that we capture any potential attacks.

23 While most of the events that have been
24 publicized have targeted retail companies and have
25 targeted the banking industry, we, in the utility

1 industry, are certainly not immune. It's just
2 we're not as high value a target at this point as
3 some of the retail companies or the banking systems
4 are today.

5 [Reference *Cyber Security Update* Slide 3]

6 The utility industry historically -- the
7 critical systems and the networks where the
8 critical systems reside -- have been disconnected
9 from the corporate networks, so it was very
10 difficult to get to those critical systems. And
11 when we speak of critical systems, we're speaking
12 of the generation and transmission assets that we
13 have at Duke Energy.

14 Currently, we are highly connected. We are
15 connected -- our critical systems are connected to
16 the corporate networks; the corporate networks are
17 connected to the Internet. While we have a layer
18 of defenses between the Internet and to our
19 critical systems, it's still a means in, if you
20 will. And certainly in the future we will see --
21 we see that the cyber-regulatory requirement is
22 going to increase. We've seen that with the NERC
23 CIP Version 5 -- which, by the way, from the
24 cybersecurity perspective, is a great thing for our
25 company and we love the controls that were mandated

1 and that we're putting in place. And the demand
2 for information is also going to increase, which,
3 again, is just more ways or vectors of attack, if
4 you will.

5 [Reference *Cyber Security Update* Slide 4]

6 From a risk perspective, a cybersecurity
7 breach is a risk to our business, in general. It's
8 something that our company has identified and it's
9 something that our company pays attention to.
10 While we identified a much larger list than I'm
11 sharing with you today of risks that we are
12 concerned with, these are the major risks that we
13 are concerned with.

14 We're concerned with loss of sensitive data.
15 We're concerned with loss of generation and our
16 ability to deliver energy. And we're certainly
17 concerned with loss of our corporate infrastructure
18 that allows us to run our financial systems, run
19 our HR system, run our outage management systems,
20 and so on.

21 The number one attack vector by far, today, is
22 phishing, and for a couple of reasons. One is it's
23 very easy to deploy. It doesn't cost a lot of
24 money; it doesn't cost a lot of know-how. It takes
25 anywhere between \$200 and \$300 for a bad guy to be

1 able to set up the ability to send over 10,000
2 e-mails a day and be able to target a person or
3 persons and try to get them to click on those links
4 and give the bad guy the ability to install malware
5 on their network and harvest data or breach a
6 network.

7 Certainly, the nation-state attackers are
8 another vector that we're concerned with. They're
9 well educated, they're sponsored, they're well
10 funded, and they're very persistent.

11 [Reference *Cyber Security Update* Slide 5]

12 And so to protect our cyberassets, we are --
13 we have a Cybersecurity Program that is implemented
14 based on the NIS Cybersecurity Framework. The
15 Executive Order 13636 that was issued by the
16 President in February 2013, ordered the Department
17 of Homeland Security to work with the private
18 sector and define a cybersecurity framework that
19 any company could easily use to protect its assets.
20 We, at Duke Energy, were involved in the process of
21 providing feedback and shaping what the
22 Cybersecurity Framework looks like.

23 The Cybersecurity Framework is made up of five
24 categories that are -- and by the way, the
25 Cybersecurity Framework is meant to be descriptive

1 and not prescriptive in nature. So, having the
2 ability to identify what our critical assets are;
3 having the right controls in place to protect those
4 assets; being able to detect an event when an event
5 happens; and -- certainly, very important -- how
6 quickly do we respond to that event; and in case we
7 have a breach, how do we recover from it. So, on
8 the next slide --

9 [Reference *Cyber Security Update* Slide 6]

10 -- I'll cover with you Duke Energy's
11 implementation of the NIS Cybersecurity Framework.
12 Certainly, from an identification perspective, we
13 know what our critical assets are, and those are
14 generation and transmission. We have sensitive
15 information that we want to protect: Our
16 customers' data and our employees' data. And we
17 conduct annually a third-party penetration test
18 that tells us what vulnerabilities we may have on
19 our network, so we address them before the bad guys
20 find them.

21 On Jeremy Carswell's team, we also have an
22 internal team that does penetration tests all year
23 'round. And, again, the desired outcome is the
24 same, and that is, to find vulnerabilities within
25 our network, address them, mitigate those risks

1 before the bad guys find them.

2 From a protection perspective, we have a
3 perimeter protection program, if you will, and it
4 consists of a defense in-depth strategy that we've
5 used for many years, and we have layers of isolated
6 networks, if you will. There are several layers
7 from the Internet all the way to what we call the
8 DMZ -- demilitarized zone -- where some of our
9 public data resides. And we have another layer
10 where our corporate infrastructure is. Then we
11 have at least one or two layers in addition to that
12 before one could get to our critical assets. And
13 between those layers we have several controls, like
14 firewalls, intrusion protection systems, and
15 intrusion detection systems. We have proxy servers
16 where we're able to look at the URLs that are
17 coming through and do some scanning on those. And
18 when we get to the most critical systems, like
19 generation and transmission, we require another
20 batch of authentication, as well, other than the
21 corporate authentication that most of the Duke
22 Energy users are using.

23 We work collaboratively with the FBI and DHS.
24 If there are threats, in general, in the utility
25 industry or industry in general or specific to Duke

1 Energy, we learn of those. We have a threat
2 intelligence team that actively works with those
3 folks, and we assess the risk to the company based
4 on those threats, and we implement controls to make
5 sure that there's not an impact on our cyberassets.

6 We have an incident response process, in case
7 an event or breach takes place. It's a
8 comprehensive one, and we exercise it at least
9 twice a year.

10 And from a recovery perspective, all our
11 systems are backed up. We have at least 30 days of
12 backup that's available in case of a total
13 disaster, and we have an annual disaster recovery
14 exercise that we run through -- and as a matter of
15 fact, we just finished one very successfully --
16 where we test our disaster recovery and we look at
17 recovering our system as if something had happened.

18 [Reference *Cyber Security Update* Slide 7]

19 So, in summary, what I'd like to leave you
20 with is that, you know, cyberthreat is both real
21 and significant in our industry.

22 We do have a comprehensive Cybersecurity
23 Program. We, on a daily basis, assess the risk.
24 We look at threat intelligence on a daily basis,
25 both from federal agencies as well as from private

1 industry. We have a Risk Management Program that
2 helps us assess the risks to our cyberassets. We
3 certainly are prepared to respond to
4 cyberincidents. And we consider regulatory
5 requirements a floor and not a ceiling for us.

6 So, with that, certainly I'll be happy to
7 address any questions.

8 **CHAIRMAN HALL:** Thank you, Mr. Myers and Mr.
9 Elabdellaoui. That was very informative.

10 Commissioners, questions? Commissioner
11 Hamilton.

12 **COMMISSIONER HAMILTON:** Both of you gentlemen
13 mentioned the incident at Metcalf. Without prior
14 knowledge that this was going to happen -- and I
15 don't want you to go into any confidential
16 information, but how could you have avoided or
17 could you avoid it today?

18 **MR. DARREN MYERS [DUKE ENERGY]:** You want me
19 to take that?

20 **MR. HAFID ELABDELLAOUI [DUKE ENERGY]:** Go
21 ahead.

22 **MR. DARREN MYERS [DUKE ENERGY]:** So, after the
23 Metcalf incident, when the industry really started
24 rallying around this, there were a number of asset
25 owners that came together to talk about the lessons

1 learned. And a member of my staff actually
2 participated in that event. I think the takeaway
3 for me was that a lot of these systems are in very
4 remote areas; it's difficult to protect against
5 everything. Resiliency is really the important
6 thing for us, but also the ability to share
7 information in a timely manner and correlate
8 incidents.

9 And I'll give you a specific outcome of
10 Metcalf. The substation had alarm systems in it
11 that were being monitored by Security, and the
12 transmission operators knew that they were having
13 equipment issues and they talked to each other on
14 the phone three times over the course of the
15 evening, but they failed to correlate the fact that
16 they were under attack.

17 So, Duke Energy is building a system operation
18 center north of Charlotte, and we've made a
19 strategic decision to locate our security command
20 center in the same building, right across the hall
21 from the system operations group. There's a
22 conference room nearby, so that when we have these
23 type of events we can work together to assess the
24 situation.

25 I also believe that putting the security

1 monitoring ability into the system operations
2 center is a best practice. We really don't want
3 the system operators focusing on security, because
4 we need them to run the bulk electric system.
5 However, when they have a Metcalf type event, we
6 should enable them by giving them access to the
7 security appliances so that they can try to make
8 that correlation.

9 **COMMISSIONER HAMILTON:** Yeah. But still, what
10 you're telling me is after-the-fact, isn't it?

11 **MR. DARREN MYERS [DUKE ENERGY]:** It is. It
12 is. You know, I sat in on a briefing in Washington
13 and there was a lot of emphasis on physical
14 security measures and what it would take to harden
15 these assets. And part of the problem that we have
16 is assets get shot at by hunters and vandals
17 routinely, and there's a long history of that.
18 This was a very coordinated attack, and all the
19 assets are technically vulnerable to that. We can
20 put measures in place to protect against a Metcalf
21 type event, but if the adversary escalates their
22 attack mechanism with a more robust tool -- like
23 ammonium nitrate and diesel fuel, for example, from
24 the Oklahoma City bombing -- then the measures that
25 we put in place to prevent Metcalf would fail.

1 It really does go to resiliency. In the ideal
2 world, we have that robust system because the
3 biggest threat to us is probably a storm. A major
4 hurricane very likely will be more impactful to us
5 than a single type event like Metcalf, where, even
6 though there were 100 rounds shot into the
7 transformers and there was \$30 million worth of
8 damage after you included the environmental impact,
9 nobody's lights went out.

10 **COMMISSIONER HAMILTON:** That's right.

11 **MR. DARREN MYERS [DUKE ENERGY]:** Okay?

12 **COMMISSIONER HAMILTON:** That's right.

13 **MR. DARREN MYERS [DUKE ENERGY]:** So, does that
14 answer your question?

15 **COMMISSIONER HAMILTON:** Yeah, I think that's
16 great. I think you answered. I guess, in the long
17 run, we need to do a better job keeping up with the
18 bad people, don't we?

19 **MR. DARREN MYERS [DUKE ENERGY]:** Yes, sir.

20 **COMMISSIONER HAMILTON:** Thank you, very much.
21 I've enjoyed your presentation from both you
22 gentlemen.

23 **CHAIRMAN HALL:** Commissioner Randall.

24 **COMMISSIONER RANDALL:** Thank you, ma'am.

25 Thank you. Good presentation. I appreciate

1 y'all being here. This could be maybe for Mr.
2 Myers and Mr. Elabdellaoui. And my question comes
3 from where I live, I guess, with being in Clinton.
4 With partners that you have with -- and I see Mr.
5 Ellerbe is giving me a real look, so...

6 [Laughter]

7 **MR. ELLERBE:** [Indicating.]

8 **COMMISSIONER RANDALL:** No. The people that
9 are co-owners, say, of nuclear assets -- and I come
10 from a Piedmont Power city. There are substations
11 there, and I think they're leased. I don't know
12 about -- I can't remember the exact thing. But I
13 guess my question is, are they part of -- the
14 people that are partners with you, are they part of
15 your security plan? And I know there's a lot of
16 communication that goes on between them and between
17 you, so I didn't know how that figured into, you
18 know, going up the channel. Are they all a part of
19 the plan, as you are both looking at it? And not
20 only physical security but cybersecurity? I think
21 -- I don't know if that was clear, or not, or if it
22 was mushy.

23 **MR. DARREN MYERS [DUKE ENERGY]:** So I can
24 address that from the physical security side. And
25 while I apologize that I don't have an example for

1 South Carolina, I can give you an example of what
2 you describe.

3 In the Midwest, we have a station that is
4 collocated with another asset owner. That asset
5 owner has responsibility for the construction and
6 the maintenance of that site. We work
7 collaboratively with them to do the assessment and
8 to validate that the results were right. But
9 because they are responsible for construction and
10 maintenance, when we get to the point that it's
11 decided that that particular asset is in-scope, we
12 intend to approach that with some type of an
13 interface agreement, and there will be some
14 information sharing as a result of that so that, if
15 they receive threat information or if we do, that
16 we're working very closely to share that in a
17 timely manner so that we can take appropriate
18 measures. Does that help?

19 **COMMISSIONER RANDALL:** Uh-huh. Thank you.

20 **CHAIRMAN HALL:** Commissioner Fleming.

21 **COMMISSIONER FLEMING:** Thank you once again
22 for being here today. This has been very
23 informative. And as you stated, you're not only
24 doing what is the standards but above and beyond
25 that, which I keep hearing over and over is most

1 important. How are you working with the
2 interdependency groups that you have, like water?
3 I understand that's a very -- well, it's very
4 critical to electricity and it's also necessary for
5 us to survive. And I understand there's a lot of
6 discussion going on there. What are you doing in
7 regards to the interdependency?

8 **MR. HAFID ELABDELLAOUI [DUKE ENERGY]:** So,
9 from a cybersecurity perspective, we collaborate
10 with the Department of Homeland Security; we
11 collaborate with the FBI; and we certainly, from
12 private industry, we collaborate with folks like
13 Dominion, like Southern, and so on. And the
14 threats at times that we see that are directed at,
15 possibly, the utility industry can be sometimes the
16 same as the water industry, and so on. So there is
17 a lot to learn that one could get from the
18 information sharing. And a lot of that really
19 comes through our work with the Department of
20 Homeland Security, for the most part.

21 **COMMISSIONER FLEMING:** And are you -- one of
22 the things I've heard in the past is that it's hard
23 to get information from the federal level. Are you
24 seeing an improvement in that? Or is that still a
25 challenge that you're working with?

1 **MR. HAFID ELABDELLAOUI [DUKE ENERGY]:** So,
2 I'll ask Jeremy to jump in if he has more
3 information to provide, but we feel that we are
4 collaborating at a level that is very adequate at
5 this point. We receive information from the
6 federal government in a timely fashion, and they
7 are eager to collaborate with us. We get timely
8 information and intelligence that we use on a daily
9 basis to protect our assets.

10 **COMMISSIONER FLEMING:** So that situation
11 sounds as if it's improved greatly.

12 **MR. HAFID ELABDELLAOUI [DUKE ENERGY]:** That's
13 correct, yes, ma'am.

14 **COMMISSIONER FLEMING:** Great. And, of course,
15 this was several years ago, but at that time I know
16 Duke was always listed as really being at the
17 forefront of security measures, both physical and
18 cyber. And it sounds like you're planning to
19 maintain that high standard of protection.

20 **MR. HAFID ELABDELLAOUI [DUKE ENERGY]:** Yes,
21 ma'am, we will continue to maintain that. We're
22 always looking for opportunities to improve our
23 security posture, absolutely.

24 **COMMISSIONER FLEMING:** And if there are breaks
25 in the security, how do you inform public service

1 commissions about them, and what is the standard
2 for that? Because I know there's a lot of secrecy
3 around that, and I'm not trying to cross any
4 barriers, but I just wondered at what stage, or
5 does it depend on the break that occurs, or --

6 **MR. HAFID ELABDELLAOUI [DUKE ENERGY]:** It
7 certainly depends on the event. We have a
8 comprehensive cyberincident response process that
9 we use. And in that process is a comprehensive
10 communication plan that we have worked with both
11 our HR Department and our Communications Department
12 to identify the folks that we would need to
13 communicate with -- both internally and externally
14 -- and have those lists available in the case of a
15 cyberevent, so that we communicate in a timely
16 fashion. So we certainly have that process in
17 place.

18 **COMMISSIONER FLEMING:** Okay. Thank you.

19 **MR. HAFID ELABDELLAOUI [DUKE ENERGY]:** You're
20 welcome.

21 **CHAIRMAN HALL:** Commissioner Howard.

22 **COMMISSIONER HOWARD:** In the regulatory
23 environment we are in, as in you're a regulated
24 industry, what kind of communication do you have
25 with ORS -- and I guess this should be a question

1 question quicker than I asked the question. Do you
2 have communications or regular meetings or reports
3 set up to communicate with not only Duke but also
4 other regulated utilities?

5 **MS. LEIGH FORD [ORS]:** We do not have reports
6 that we've been receiving. We have been monitoring
7 everything that's been required in the new
8 standards that are coming down, and have had in-
9 person as well as electronic communication with the
10 utilities. But anything in particular as far as a
11 report, we do not have at this point.

12 **COMMISSIONER HOWARD:** Well, thank you.

13 **MS. LEIGH FORD [ORS]:** You're welcome.

14 **CHAIRMAN HALL:** Commissioner Fleming has a
15 question, as well, for Ms. Ford. Ms. Ford -- I'm
16 sorry, Commissioner Fleming has a question for you,
17 as well.

18 **MS. LEIGH FORD [ORS]:** Yes, ma'am.

19 **COMMISSIONER FLEMING:** I just wanted to follow
20 up on that. Do you have cybersecurity specialists
21 on staff at ORS?

22 **MS. LEIGH FORD [ORS]:** We do not. At this
23 point, I don't think there's been a need for it,
24 but if it is something that we would need, we might
25 engage an outside consultant. We do have one

1 person in staff who deals with the cybersecurity
2 for the agency and all of the state requirements,
3 but something, you know, specific to this, we do
4 not.

5 **COMMISSIONER FLEMING:** Okay. Thank you.

6 **MS. LEIGH FORD [ORS]:** Uh-huh.

7 **CHAIRMAN HALL:** Commissioner Whitfield.

8 **VICE CHAIRMAN WHITFIELD:** Thank you, Madam
9 Chairman.

10 Thanks to both of you for your presentation.
11 I do have an one quick question. I guess it would
12 be for you, Mr. Myers, because it relates to
13 physical security. In discussing NERC CIP-014 --
14 and I know you stated you had someone from the
15 company, from DEC or DEP, representing the company
16 I guess in the development of that standard,
17 somebody at NERC that was involved, and you had
18 your slide with the timeline on it. And it sounds
19 like, in correlation with your plans and so forth,
20 that you are, at least -- I know you're obviously
21 aware of the timeline, but it looks like your plans
22 seem to follow that. Do you anticipate any
23 problems meeting the October 1, 2015, deadline or
24 for all requirements in December 2016? Or do you
25 think you'll be ahead of that? Where -- maybe you

1 said that in your presentation but somehow I missed
2 exactly where the company was, in compliance.

3 **MR. DARREN MYERS [DUKE ENERGY]:** I do not
4 believe that we'll have any difficulty at all
5 meeting the timeline. Whether we select to submit
6 early, I can't answer that, because we really don't
7 have the final list of assets yet.

8 The asset base that we're modeling from, it
9 meets -- it's based off of the risk-based
10 methodology that's used for the other CIP
11 standards, as a starting point, and then the
12 requirements you saw on the slide about the
13 voltages and the number of connections. So we know
14 what our starting list is and we have a relatively
15 short list that is being discussed for
16 consideration. We don't see this to be a
17 significant number, and I think that will work well
18 for us in meeting the timelines to complete, not
19 only of the electric system analysis but the
20 vulnerability assessment, and develop the plans for
21 whatever measures we intend to take.

22 Now, when I talk about measures, we're
23 exploring a lot of things with our industry
24 partners that I mentioned at EPRI and the
25 Transmission Forum. There's a lot of benchmarking

1 in the industry across the utilities to talk about
2 approaches to this. Another potential approach is
3 to buy more spare equipment, to change the makeup
4 of the electric system so that no single asset
5 becomes extremely important to the reliability of
6 the bulk electric system.

7 So I, personally, as a security person, don't
8 recommend that we build large concrete walls and
9 create a Jericho around our assets. I recommend
10 that, where we have those potential single points
11 of failure, that we harden the infrastructure,
12 because it will serve us well, regardless of what
13 the threat is. Does that answer your --

14 **VICE CHAIRMAN WHITFIELD:** Yeah, and you're
15 saying have backup transformers and things of that
16 nature, rather than build a fortress, so to speak.

17 **MR. DARREN MYERS [DUKE ENERGY]:** That's
18 correct.

19 **VICE CHAIRMAN WHITFIELD:** And I guess -- and
20 my question to you, you know, is not to go where
21 the former FERC commissioner went in talking about
22 specific assets in certain substations, but the
23 overall timeline, I guess you don't foresee any
24 issues there with the companies -- both DEC and
25 DEP?

1 **MR. DARREN MYERS [DUKE ENERGY]:** I predict,
2 for certain, we will be in compliance with the
3 requirements.

4 **VICE CHAIRMAN WHITFIELD:** All right. Thank
5 you, sir.

6 That's all I have, Madam Chairman.

7 **CHAIRMAN HALL:** Commissioner Elam.

8 **COMMISSIONER ELAM:** Thank you.

9 For me, as well, thank you both for being
10 here. It's been interesting. You mentioned during
11 your presentation that you had an internal team
12 working on some penetration studies of the systems.

13 **MR. HAFID ELABDELLAOUI [DUKE ENERGY]:** Right.

14 **COMMISSIONER ELAM:** Are you doing that just
15 internally, or are you doing any reaching out to
16 someone external, like Black Hat type of guys that
17 I know help a lot of corporations judge their
18 vulnerabilities?

19 **MR. HAFID ELABDELLAOUI [DUKE ENERGY]:** So, we
20 use professional companies. We use external
21 entities that can give us an opinion of how well
22 we're doing, both internally and externally, and we
23 use them -- we provide them with a scope of work
24 that they need to do, and we allow them to go do
25 penetration testing and give us that independent

1 view of our cybersecurity posture.

2 The folks we use internally are Duke Energy
3 employees.

4 **COMMISSIONER ELAM:** Right.

5 **MR. HAFID ELABDELLAOUI [DUKE ENERGY]:** And the
6 Duke Energy employees are well educated in the
7 arena of penetration testing. And those folks are
8 looking at it all year 'round and they have
9 different scopes, depending on where we see some of
10 the risks may be, and so on.

11 Related to Black Hat --

12 **COMMISSIONER ELAM:** Well, I just know that's
13 like, from what I understand, an annual convention
14 of --

15 **MR. HAFID ELABDELLAOUI [DUKE ENERGY]:** It --

16 **COMMISSIONER ELAM:** Some corporations really
17 have reliance on those folks.

18 **MR. HAFID ELABDELLAOUI [DUKE ENERGY]:** So, we
19 do send folks from our cybersecurity organization
20 to the Black Hat conference.

21 **COMMISSIONER ELAM:** Okay.

22 **MR. HAFID ELABDELLAOUI [DUKE ENERGY]:** They go
23 and get educated on the latest threats, on the
24 latest ways to penetrate networks, and so on. We
25 learn from those and apply them inside of our

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

network.

COMMISSIONER ELAM: Is a non-Internet-connected network feasible for critical infrastructure like this? Or am I too close to something?

[Laughter]

I saw Mr. Ellerbe --

MR. HAFID ELABDELLAOUI [DUKE ENERGY]: It's a philosophical question.

COMMISSIONER ELAM: Okay.

[Laughter]

The last time I had Philosophy was in college, and it was a really, really strange class, so I'll stop.

COMMISSIONER HAMILTON: I think you just had another course.

CHAIRMAN HALL: Commissioners, any more questions?

[No response]

Our attorney has a question for you.

MR. MELCHERS: Thank you, Madam Chairman.

Quick question about your "Jericho" comment. It sounds like at least two of the options that you've presented to us today are redundancy or hardening, and I'm curious which has a greater

1 impact on ratepayers.

2 MR. DARREN MYERS [DUKE ENERGY]: I can
3 describe our approach, and maybe that will help.
4 We have substations at our nuclear stations, and we
5 have armed security officers there that have the
6 statutory authority to use deadly force. So, if
7 those happen to be in-scope and we have those
8 measures in place, the hardening that we do there
9 would be potentially less than a very remote
10 station where the law enforcement response was
11 significantly delayed because of its remote
12 location. And where they stand alone in very
13 remote areas, we will need more time to detect. So
14 we want to delay anyone from getting in or shooting
15 at the assets; we want to detect that; we want to
16 notify law enforcement to begin the response to
17 that. And we want the system operators to be aware
18 of that so that they can begin executing a plan to
19 switch around that asset to prevent outages.

20 So, each asset really has to be looked at on a
21 situation-specific basis, and we'll need to
22 understand not only the vulnerabilities to that
23 station but the response time to that, and we'll
24 have to weigh the costs of the measures against the
25 costs of spare equipment or redundancy, and then

C E R T I F I C A T E

I, Jo Elizabeth M. Wheat, CVR-CM-GNSC, do hereby certify that the foregoing is, to the best of my skill and ability, a true and correct transcript of all the proceedings had and testimony adduced in an Allowable Ex Parte Proceeding held before THE PUBLIC SERVICE COMMISSION OF SOUTH CAROLINA in Columbia, South Carolina, according to my verbatim record of same.

Given under my hand this 18th day of December, 2014.



Jo Elizabeth M. Wheat, CVR-CM/M-GNSC
Court Reporter