

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

BEFORE THE
ILLINOIS COMMERCE COMMISSION
CYBER SECURITY POLICY SESSION AGENDA
Thursday, July 21, 2016
Chicago, Illinois
Met, pursuant to notice, at 10:00 A.M.,
at 160 North La Salle Street, Chicago, Illinois.

PRESENT:

- BRIEN J. SHEAHAN, Chairman
- ANN MCCABE, Commissioner
- SHERINA E. MAYE EDWARDS, Commissioner
- JOHN R. ROSALES, Commissioner

SULLIVAN REPORTING COMPANY, by
PATRICIA WESLEY
CSR NO. 084-002170
And
CHRISTA YAN
CSR No. 084-004816

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

AGENDA

MODERATOR:

MS. ANNE McKEON, Legal and Policy Advisor,
Office of Energy Infrastructure Security -
FERC

PANELISTS:

MR. ROBERT IVANAUSKAS, Attorney-Advisor,
Office of Energy Infrastructure Security -
FERC

MR. KIRK LONBOM, Chief Information
Security Officer - State of Illinois

MS. TINA HAURI, Chief Information
Security Officer - City of Chicago

MODERATOR:

MS. NAKHIA CROSSLEY, Advisor -
Illinois Commerce Commission

PANELISTS:

MR. WILLIAM LUCAS, Director of
Technology Security and Compliance -
WE Energy

MR. NICHOLAS SANTILLO, Vice President,
Internal Audit and Chief Security
Officer - American Water

MS. MARY P. HEGER, Senior Vice President and
Chief Information Officer - Ameren

MR. JOHN GOODE, Chief Information
Security Officer - MISO

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

AGENDA

MODERATOR:

COMMISSIONER SHERINA MAYE EDWARDS

PANELISTS:

MS. JENNIFER RATHBURN, PARTNER/CO-CHAIR,
Data & Privacy & Security Team -
Quarles & Brady

MR. BOB LOCKHART, Manager,
Cyber Security Programs - Utilities
Telecom Council

MS. SHARLA ARTZ, Director of Government
Affairs, Schweitzer Engineering
Laboratories, Inc. - United States
Energy Association

MS. ANNABELLE LEE, Principal Technical
Executive, Cyber Security Power Delivery
and Utilization - Electric Power Research
Institute

1 COMMISSIONER MAYE EDWARDS: Good morning,
2 everyone. Good morning. Illinois Commerce
3 Commission. For many of you, welcome to the windy
4 and hot City of Chicago. We are extremely excited
5 to present today's policy session regarding cyber
6 security as it relates to the critical energy
7 infrastructure.

8 This session is convened pursuant to
9 the Illinois Open Meetings Act, and our guests and
10 panel should be aware that a court reporter is
11 present. A transcript of this session, along with
12 copies of the presentation, will be posted to the
13 Commission's website.

14 With us today are Chairman Sheahan,
15 Commissioner McCabe -- and Commissioner del Valle is
16 not present today -- excuse me -- and Commissioner
17 Rosales, but we do have a quorum.

18 On behalf of the ICC and my fellow
19 Commissioners, thank you all for joining us, a
20 special thanks to our panelists for their
21 willingness to participate and lend their expertise
22 to this session. We look forward to hearing from

1 all of you today.

2 Now there is absolutely no question
3 and no doubt about it that the Internet has
4 revolutionized the way that we conduct business and
5 the way that we live our lives. It is an extremely
6 powerful tool and has met virtually every aspect of
7 the modern world from one-on-one interactions to
8 worldwide databases and everything in-between;
9 however, the vast capabilities of the Internet can
10 also be used as a dangerous weapon. Cyber attackers
11 are considered by many to be more threatening than
12 physical attacks because they are more likely to
13 occur without being detected.

14 Additionally, cyber criminals are not
15 physically present and do not have physical
16 addresses, which, obviously, makes it difficult to
17 apprehend them and locate them. We see some of
18 these issues play out in several recently high
19 profiled breaches throughout the retail and
20 financial industries.

21 I'm sure many of you heard that just
22 last week a congressional report came out saying

1 that China was likely hacking the FBI for three
2 years. All of these incidences go to show that
3 cyber security is a concern across all industries
4 and all sectors and that absolute security is an
5 absolute myth, because our nation has become reliant
6 upon luxuries that electric, water, sewer, natural
7 gas, petroleum, telephone and Internet provide,
8 hackers, cyber terrorists and enemies of the U. S.
9 realize how much we depend on these resources and
10 they also recognize that a coordinated and large
11 scale attack on our critical infrastructure could
12 cripple our nation. The devastating effects of the
13 December 2015 Ukrainian power outage serve as a
14 stark warning in this regard.

15 Traditionally, state public utility regulators
16 have not been incredibly involved in cyber security
17 efforts. Most of the recent action have taken place
18 at the national level, beginning with President
19 Obama's 2013 Executive Order 13636. This Order
20 recognizes the threat to critical infrastructure as
21 one of the most serious national security challenges
22 and its stress of the importance of protective

1 security standards, and there are also several
2 national entities and agencies responsible for
3 implementing and overseeing cyber security
4 regulations, and we'll hear about some of these
5 things today.

6 Now, as a state regulator here in
7 Illinois, I have taken great interest in cyber
8 security as it relates to the critical utility
9 infrastructure, and I know that my fellow
10 Commissioners and our ICC Staff work extremely hard
11 to follow the threats, trends and best practices
12 related to this important issue.

13 Additionally, over the past few years,
14 the National Association of Regulatory Utility
15 Commissioners, also known as NARUC to some of you,
16 has repeatedly charged state commissioners to take a
17 larger leadership role in protecting critical
18 infrastructure from cyber attacks.

19 I do believe that the Commissioners
20 are in a unique position to help combat the
21 increasingly sophisticated cyber attacks through
22 coordinated dialogue and efforts across the entire

1 energy industries, including government officials,
2 policy makers, regulators, law enforcement, and
3 utility representatives, and private sector
4 stakeholders.

5 Now the purpose of today's session is
6 really to do just that, to bring together these
7 great key stakeholders for a discussion of what has
8 been done, what needs to be done, and how we can
9 work together to accomplish the important goal of
10 protecting critical utility infrastructure from
11 potentially devastating cyber attacks.

12 We have invited representatives from
13 all levels of government to discuss ongoing
14 enforcement and coordinating efforts at the
15 national, state, and local levels.

16 We will also hear from utility
17 information security officers about how they're
18 protecting their critical assets and preparing for
19 possible threats.

20 Finally, we will discuss strategies
21 for implementing best practices with industry
22 experts who are well versed in cyber security

1 collaboration both among government agencies and in
2 the government sector and the private sector are so
3 critical.

4 So I'll begin by bringing into the
5 equation our panelists. Each panelist will have
6 about five to ten minutes to expand on my
7 introduction to supplement more about their role and
8 what their agencies do in terms of cyber security.
9 We will then go into our question-and-answer
10 session, which I encourage the Commissioners and
11 Chairman to chime in whenever they have questions or
12 comments.

13 So our panelists are Robert
14 Ivanauskas, Attorney-Advisor, at the Office of
15 Energy Infrastructure and Security at FERC; Kirk
16 Lonbom, Chief Information Security Officer with the
17 State of Illinois; and Tina Hauri, Chief Information
18 Security Officer for the City of Chicago. Thank you
19 all for being here today.

20 Robert, why don't you go first and
21 tell us a little bit more about FERC's Office of
22 Energy Infrastructure Security and your role there.

1 MR. IVANAUSKAS: Well, I'm really glad to be
2 here, because actually I probably haven't been in
3 this room maybe 20 years. I'm a Chicago native and
4 I moved out to the Washington, D.C., area 15, 16
5 years ago, and it's great to be sort of back in this
6 room and talking about issues that are important to
7 the State of Illinois, which is where most of my
8 family still lives and where my true home and heart
9 is, but, anyway, being from the federal government,
10 I work at FERC, which is an independent commission
11 composed of up to five commissioners and probably
12 the same with the Illinois Commission.

13 What I say -- and what I say or even
14 if I promise something, none of that can bind the
15 Commission, and that's really important, not because
16 it sort of like the generic thing that speakers
17 always say, but it's important because it allows the
18 federal government to have really a collaborative
19 dialogue with people out in the public who are
20 interested in this topic, and so because I can go
21 out there and other people from our Office of Energy
22 Security can go out into the public and talk through

1 these issues and not bind some of the commissioners
2 or the federal government, so that really allows a
3 good two-way communication that allows a discussion
4 of potential threats, potential vulnerability on the
5 power grid and throughout the energy infrastructure.

6 So that's really good news, and I also
7 wanted to start off with a little bit more good news
8 though. I'm moving offices. I'm going from like
9 one office carol to another office carol in my
10 building, so there's no big deal, but I have to pack
11 up all these old boxes.

12 So as I'm packing up the old boxes, I
13 noticed I have got a stack of old magazine articles
14 about cyber security and the energy grid, and I'm
15 looking at them and I start reading them, and it
16 sounds exactly like the discussion that we so far
17 have today where it's an important issue, and we
18 have got to take a good hard look at things, and we
19 have got to start moving forward, and we have got to
20 make sure that we are ready for whatever may happen,
21 and that's really good news, that Article in 2002 is
22 the same as today because that means that we have

1 been handling this issue for a long time. We have
2 been looking at it, and also it means that there
3 fundamentally hasn't been big disasters in this
4 arena.

5 Now, of course, that doesn't mean that
6 tomorrow won't be different, but it does mean that
7 the industry, government, state, local, federal,
8 have been dealing with this issue for a long time,
9 but actually it goes further back than the year
10 2002.

11 If you go back to 1940, 1945, this
12 was -- energy infrastructure was one of maybe the
13 most critical issues in the Second World War and the
14 Federal Power Commission at the time, which is the
15 predecessor of FERC, was heavily involved with
16 advising the states, advising industry on ways to
17 protect the grid.

18 The grid at that time was mostly an
19 oil pipeline industry grid, and it was a little bit
20 behind the electric grid, and there was a lot of
21 electric coordination, there was protecting the
22 power plant, a lot of work was done, back in those

1 days, it was top secret.

2 Today the top secret sort of documents
3 are no longer that, because 60, 70 years have past.
4 So if you go look at those documents, you will see
5 that they sound a lot like the types of things that
6 we are dealing with today, and so that sort of got
7 me interested in other historical stuff.

8 I'm in my office building, and there's
9 this old library, and I see this book. It says
10 "Preparing for the Electricity Grid and the War,"
11 and it's a real thick book, old book, so I open it
12 up and I thought it was about World War II. No,
13 it's about World War I. It's all about the efforts
14 in World War I for the industry to make sure that
15 the power grid was protected and was able to produce
16 enough electricity for the war effort actually,
17 literally one hundred years ago.

18 So this is not a new issue. This is
19 an issue that the nation has faced for a long time,
20 and, of course, evolves because the threat actors
21 evolved, and that's why we are evolving. That's why
22 we are having this discussion.

1 So FERC itself -- maybe I should say
2 FERC's role is in the federal government. So we
3 have all sorts of different federal agencies that
4 deal with this issue from the military and
5 intelligence community, and that's what you probably
6 see in the newspapers more often, but then on the
7 energy side you have FERC, the Department of
8 Homeland Securities on the energy side and the
9 Department of Energy.

10 All of those three agencies, plus a
11 few more, have some pretty sophisticated programs
12 that are getting a lot better every day and right
13 now the latest trend is in sharing, sharing
14 indicators of problems, let me put it that way, and
15 perhaps the easiest example is the DHS Program.
16 It's called the AIS Program, and this stands for
17 Automated Indicator Sharing, and that comes out of
18 the recent Cyber Security Act which allows private
19 entities and the public to share information with
20 the government and have that information.

21 So let's say a private company gets
22 attacked in some way through e-mail, that company can

1 send that information to DHS and immediately DHS can
2 circulate that information out to the rest of the
3 public, so it's not a -- DHS doesn't wait a day or
4 doesn't wait two hours to circulate that app. The
5 idea is to try to immediately send out information
6 about these so they can be blocked quickly.

7 One thing about the computer age and
8 telecommunications what they are today is that it
9 happens so immediately that the bad guys, when they
10 attack, they can attack with very low cost across an
11 entire network -- across an entire industry or
12 across an entire nation and the speed at which they
13 can attack means that you need speed to respond to
14 those attacks, and that's what the Automated
15 Indicator Sharing is all about, and those types of
16 programs are really rolling out right now. They
17 were in their infancy a few years ago and now we are
18 finally getting the chance to test, them to develop
19 them, and to bring a lot more people into the
20 communities.

21 The way I look at it is a little bit
22 like the neighborhood watch program where everybody

1 on the block is sort of watching out for the bad
2 guys, and you have one guy whose home is broken
3 into, and then if that information can immediately
4 go to the police and the police can immediately send
5 that to everybody else on the block, good things can
6 happen. You can stop the home burglaries much more
7 quickly if a certain neighborhood watch, and this is
8 sort of the neighborhood watch on a nationwide scale
9 and potentially at some point even further.

10 There's a lot of exciting things and
11 I'm looking forward to talking to you today, and
12 thanks for inviting us to come to Chicago.

13 MS. McKEON: Thank you, Robert.

14 Kirk, could you tell us a little bit
15 more about your role as the CISO of the state and
16 maybe touch on how in recent years that role wasn't
17 filled, at least not full time. Tell us about how
18 significant that is for the State of Illinois.

19 MR. LONBOM: Yes, I would be happy to. Thanks
20 for the opportunity to meet with you today. I have
21 had an opportunity to meet with some of you through
22 our partnerships.

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

(A brief pause.)

My first day at the microphone. How is that.

My name is Kirk Lonbom and I am the Chief Information Security Officer for the State of Illinois. Anne is correct, the role of the CISO of the state has not been well defined until recently. Previously the role of the CISO was pretty much over the Central Management Agency of the state which is focused -- the agency who had a centralized data center, et cetera. Other agencies were essentially on their own.

I served as a deputy to the CIA for the Illinois State Police for about eight years, the Illinois Emergency management for five prior to taking this position, and we were essentially on our own. We did our own policies. We did our own protection. We did our own cyber defense. We did our own everything, and with this new administration part of our transformation with the state, the role of CISO has been redefined into a much larger role. I'll tell you a little bit about the transformation

1 of the state and how the CISO ties into that, the
2 role of the state, and talk a little bit about what
3 we are doing and where we would like to go.

4 In terms of transformation of the
5 state, those of you who live in Illinois you
6 interact with the State of Illinois and try to do so
7 electronically you probably have a lot of problems.
8 We have a lot of obsolete systems. It takes a lot
9 of work to do business with the state. We're
10 working to fix that for the citizens through
11 transformation of our technology.

12 We have probably 45 years of
13 legacy technology, some of which is still in
14 production, and so we have a very aggressive agenda
15 in terms of digitizing capabilities of state
16 government to protect the systems and server
17 systems.

18 We have several data initiatives.
19 It's mobile. It's Cloud. It's Internet of things.
20 It's data and it's security.

21 As we make this transformation with
22 the changing threats and ever-growing risk, we have

1 a big job in terms of both modernizing our
2 technology and trying to keep up with security
3 protection that we see apply.

4 So the role of the CISO was created
5 and essentially my role is now information cyber
6 security policy and operations for all agencies that
7 operate under the governor. It's kind of like we
8 are going through this massive corporate merger of
9 dozens and dozens and dozens of agencies bringing
10 them together into a single IT organization and
11 infrastructure, and I must say the challenge is
12 somewhat daunting.

13 We have many concerns about increasing
14 threats from nation states. We will always be
15 attacked by the criminal element, the hackers, et
16 cetera. Some of you may have heard of the group
17 Anonymous who will take some type of topic and
18 essentially attack states or governments whether
19 it's unrest regarding police shootings and violence
20 and things of that nature or whether it's regarding
21 political issues, so we are hit from all sides, and
22 what we are attempting to essentially build that

1 infrastructure and that capability best to protect
2 the state.

3 We have a vision for not just
4 protecting state agencies but essentially a vision
5 for helping Illinois be the best cyber security
6 state in the nation. I think that's not only going
7 to be common, it's not only going to be for
8 citizens, it's going to be for the safety of our
9 citizens. It's just overall best for all of us.

10 We are working towards an overall
11 cyber construction plan, which would join entities
12 such as the private sector and public sector in
13 terms of being able to respond to cyber destruction.

14 As CISO, we have somewhat of challenge
15 in that when security incidents occur some of them
16 are local, some of them are within a particular
17 agency or limited, but some can be widespread, and I
18 think that's what we are talking about when we talk
19 about cyber destruction attacking the utility
20 industry.

21 At a certain point cyber destruction
22 goes beyond the role of the CISO and becomes a part

1 of the Illinois Emergency Management Response, so we
2 are working with private sector and public sector
3 entities to develop overall cyber construction for
4 the state.

5 I want to comment a little bit on what
6 Robert talked about, information sharing. The
7 Information Sharing Act has really helped open up
8 the potential for information sharing. We are
9 looking to participate in the AIS program. We have
10 partnerships with private sector. For example, we
11 have the government established Technology Advisory
12 Committee made of the private sector corporate
13 sponsors and personally performing mentoring with
14 the CISCOs from agencies like State Farm and
15 Caterpillar, and we are continuing to exchange
16 information regarding that.

17 I think one thing that we have to our
18 advantage overall is that in the information sharing
19 arena we all recognize that we have a common
20 problem. I worked in the intelligence arena during
21 9-1-1 and I can tell you that prior to 9-1-1 the
22 information sharing across the intelligence

1 community and the law enforcement community was
2 pretty sparse.

3 I actually worked three years in an
4 undercover role and I can tell you the trust not
5 only between the offenders and informants but also
6 between the police was not the best.

7 I could tell you the cyber arena that
8 has drastically changed. We have a recognition that
9 we all must attack this problem together and work
10 together to share this information.

11 MS. McKEON: Thank you very much, Kirk.

12 Tina, could you talk about your role
13 as CISO for the City of Chicago and perhaps touch on
14 how common it is for the city to have its own CISO.

15 MS. HAURI: Yes. Thank you. Good morning and
16 thank you for allowing me to be here and be a part
17 of this discussion and collaboration.

18 The comments made by Robert and Kirk
19 both resonate with the city and bring it down to the
20 local level where we have the responsibility as the
21 city to protect the citizens, the information that
22 the citizens share with us in the course of their

1 everyday business, and you all -- excuse me -- the
2 city website you notice we're offering more and more
3 of the services for payments electronically which
4 creates a much larger footprint for us to service.

5 I have been with the city about two
6 months now. I am the third CISO in four years for
7 the City of Chicago, so there's some great
8 groundwork that's been laid before me by way of a
9 strong policy and some strong -- I'm just going to
10 say -- broadly technology controls to help us
11 protect, and detect, and monitor the city's systems
12 that are serving our citizens.

13 We are looking forward to
14 collateralizing with Kirk, with federal agencies and
15 in order to be efficient. Part of our challenge as
16 a city is the resources that we have both from a
17 capital perspective and a system perspective are
18 scarce.

19 Resources is a big economic problem,
20 and so as I'm looking ahead to how we need to serve
21 and grow, one of those challenges will be the
22 resources to continually manage the processes to

1 protect the information. These are not one-and-done
2 kinds of initiatives to support NIST or to support
3 our policies that we have based our program on.

4 Our Department of Innovation
5 Technology continues to consolidate the system and
6 try to become more efficient at every chance we can,
7 but with that, there's still the high level
8 requiring to protect the system and the information
9 that is entrusted to us by our citizens.

10 Kirk has mentioned -- Robert has
11 mentioned the threat actors. They're busy; they're
12 well organized; they're well funded; and the city,
13 because of many things that have gone on, is, in
14 fact, a target of many of these bad actors, so we do
15 have our hands full keeping an eye on the system in
16 the prevention and detection and response, so our
17 ability to actively respond, aggressively respond
18 and accurately respond when we do have an incidence
19 is also something that I will be turning a key eye
20 towards so that we can minimize any impact that we
21 would see as a city.

22 Moving forward, again collaboration is

1 key across our interdepartmental government
2 agencies, but I think there are significant
3 opportunities to partner with the private sector.

4 I come from private sector and there
5 have been regulatory statutes in place for a number
6 of years that have required the private sector to
7 take strong strides to the program, protecting
8 information, working with third-party vendors that
9 service our systems, processes, and citizens.

10 I think there's much we can learn from
11 private sector and bring into the government to help
12 shorten our time lines to be successful in
13 supporting our own policies. We're long on policy.
14 Policy is sometimes challenging to write, because of
15 the different interests that have to be served in
16 writing the policy, but the bigger challenge then
17 becomes how do we manage to the policy that we set
18 forward.

19 Again, many of the requirements that
20 the policy set forward are day-to-day. Every one of
21 our 36,000 employees has a responsibility to support
22 some facet of the information that serves the City

1 of Chicago.

2 So, again, as we write policy, we have
3 to consider the mandates, the personnel, the
4 systems, and the funding that are necessary today,
5 tomorrow, and in the future, to support that policy.
6 It's not a -- the majority of what we have to do is
7 every day 24 by 7 by 365 because the bad actors
8 don't sleep.

9 We are well organized. We are on
10 every continent. We have redundant systems that
11 would make our eyes water. They are well staffed.
12 They are not short of people who have different
13 agendas who want to disrupt and they want to make
14 money.

15 Four hundred billion dollars is the
16 cyber crime number last year. That's how much money
17 they made. They made that by stealing it from
18 legitimate government agencies, businesses, and
19 individuals. They're busy. They're organized.
20 They want our money. They want our information so
21 they can use it to sell to make money, and, again,
22 it's our responsibility up here, our and our teams,

1 to put in place a system, processes, education
2 awareness, to do our very best to protect what we're
3 entrusted with. Thank you.

4 MS. McKEON: Thank you all for those
5 introductions, and, Tina, you led nicely into my
6 first question, which is about technology and how
7 bad actors are getting more sophisticated.

8 COMMISSIONER ROSALES: Can I ask a question.

9 MS. McKEON: Oh, please. Yes.

10 COMMISSIONER ROSALES: I'm sure we'll get into
11 this later on throughout the day. There seems to be
12 some degree of malicious activities. Sometime it's
13 to gather information. Sometimes it's just to take
14 down the system.

15 So I wanted to ask both Tina and Kirk
16 from the citizen and state perspective do you have
17 mock drills in which you intentionally try to hack
18 into your systems and what's the frequency that this
19 occurs if you do have them?

20 MS. HAURI: Having been here two months, we have
21 not had any in my initial tenure, but we will.
22 They're called tabletop exercises in our vernacular,

1 and I am intending for us to have them.
2 We're across 30 departments in six sister agencies
3 as representing the City of Chicago site reference,
4 so I do work with Cook County. There's an
5 enter-agency group that I've met once with already.
6 There will be an exercise in October with that
7 group, but, as a city, we do need to have them.
8 They are important. I have chaired them in previous
9 lives of mine.

10 They do reveal a lot. They let us
11 know that our preparations may not be nearly as
12 detailed and effective as we thought they were, so
13 they help us identify areas for improvement within
14 our own organization, whether it be a systems issue,
15 also collaboration that helps us understand where we
16 don't have the right relationships already in place
17 to respond appropriately to an emergency.

18 So they're important. They will be
19 happening. I do not have the schedule for them as
20 of right now, but please come back to me soon and I
21 will be looking into a strategy, but they're
22 important. They're necessary and they will be

1 happening.

2 MR. LONBOM: That's a great question. We do at
3 several levels. One is at a tactical level. One of
4 the things that I think those in securities have
5 found that security is often an afterthought, when a
6 system is developed, we have to change that, and
7 essentially securing the system from soup to nuts in
8 terms of system development and solution
9 development.

10 So, as every new system is set up, we
11 do more and more of that at the Cloud because
12 providers are more Cloud-based instead of their own
13 system, and software, and service, and that sort of
14 thing.

15 We will also use something more of a
16 broad test. For example, we'll be going in
17 testing -- penetration testing, again
18 infrastructure. We're doing that across all of
19 these agencies. We're doing this merger lift, if
20 you will, as we find out what our vulnerabilities
21 are, et cetera.

22 From a state-wide level, we do that both

1 internal with our own internal hackers. I have got
2 some good scary hackers that work with me, so we do
3 that internally as well, and on the state's
4 infrastructure, and which is very critical. We
5 provide network services, not just to state
6 agencies, but out of schools and municipalities
7 throughout our central network, so we do that both
8 internally with our own guys but also working
9 towards a external penetration test.

10 Something I would like to share is the
11 Department of Homeland Securities has an array of
12 programs that they offer for free in terms of cyber
13 protection. One of their programs is they work with
14 government agencies and industry to do cyber tests.

15 We are looking to see how our
16 employees react to penetration tests of wireless, so
17 that's something that we are working on the schedule
18 for us. It's a kind of a six-month waiting list
19 that's actually is a great service. For the private
20 sector, we recommend that third-party penetration
21 tests should be done on our own businesses.

22 COMMISSIONER ROSALES: Thank you.

1 MS. McKEON: Chairman, Commissioner, any other
2 questions at this time?

3 (No response.)

4 Great. Well, Robert, you mentioned
5 that this is not a new issue. It's been around
6 since the 40s. You mentioned recently finding an
7 article from 2002 about the same issue, but I think
8 you all touched on the threat actors are constantly
9 evolving and the landscape is constantly changing.

10 So how can government actors ensure
11 that their regulatory and enforcement efforts are
12 keeping up with these constantly changing threats?

13 MR. IVANAUSKAS: I think for me to start on this
14 one from the regulatory angle, and so at FERC our
15 history of energy security is really intertwined with
16 our history of reliability, and that history most
17 closely begins at the FERC side after the 2003
18 blackout where pretty much a lot of New York State,
19 and Ohio, and a little bit of Michigan all went
20 blacked out.

21 After that, there was a law passed
22 in 2005 which eventually led to mandatory standards

1 at NERC on the electric power grid, the bulk power
2 system, so those mandatory standards include cyber
3 security standards on the bulk power system.

4 Since those are enforceable, that
5 means that an electric utility can get a penalty
6 from -- assessed by NERC and imposed or approved by
7 FERC, and that can make an electric utility, because
8 of the possibility of a penalty, that could make an
9 electric utility hesitant to come to FERC with
10 questions about deeper threats than just the types
11 of threats that can be stopped with the cyber
12 securities standards of NERC.

13 So because of that, our chairman at
14 the time, Jon Wellinghoff, wanted to remove the sort
15 of a voluntary collaborative function of FERC from
16 the enforcement function, and that's really the
17 genesis of the creation of the Office of Energy
18 Infrastructure Security, and so that that office,
19 OEIS, where I work, our idea is to work
20 collaboratively, to work confidentially with
21 electric utilities, to the extent we can, based upon
22 public access laws and talk through a lot of those

1 issues in a place where there isn't a continuous
2 constant risk of if you talk to a federal agency,
3 well, then there is a very good chance that somebody
4 somehow might some day get interested in an
5 enforcement action.

6 So the regulatory landscape is
7 continuously changing, and right now we're at the
8 point where we have our Office of Electric
9 Reliability, which focuses on the NERC standards,
10 and we have the Office of Energy Infrastructure
11 Security, which doesn't. It focuses more on the
12 threats and communicating with the industry on the
13 best ways to address those things.

14 MS. HAURI: From the city's perspective, it is
15 the undertake projects that touches the city's
16 infrastructure. We are issuing requirements for the
17 third parties through the RFP process and assessing
18 the capabilities of those that would be working with
19 us to provide these services.

20 The majority of these services include
21 infrastructure, heavy cyber components, whether it's
22 Cloud-based services, as I first mentioned, or

1 electrical. There are sensors and devices being
2 added to most services that we use today. That
3 means there's a cyber security component to those
4 projects, even though it looks like a Streets and
5 San initiative or electrical initiative, so my team
6 is engaged in a couple of projects right now. We'll
7 continue to be engaged and continue to work to make
8 certain we understand how the city is connecting and
9 who is overseeing the connections that we make that
10 serve our city's infrastructure.

11 It will be ongoing. Again, this is
12 part of that 24/7, 365, and in perpetuity. Again,
13 the system will out live most of us, transcend and
14 be in place long after many of us have moved on to
15 the next chapter in our lives, so we also need to
16 look ahead to make sure we understand what the
17 tomorrow may look like and how things can be
18 maintained going forward.

19 MR. LONBOM: Thanks for quoting those facts to us
20 to keep up with things. So as you talk about -- we
21 talked a little bit about the regulatory side and
22 the state's perspective to impact by all sorts of

1 regulatory type of issues, compliance matters,
2 whether it be federal income tax data, PCI, credit
3 card information, et cetera.

4 Just to comment on all this
5 connectivity, the world is moving very quickly. We
6 all heard the talk about the Internet of things in
7 connecting the world.

8 I was thinking that I had protected
9 myself pretty well in that I had the Internet of
10 things and I stood on my record scale that feeds my
11 cell phone, and I didn't realize that I actually was
12 connected but I wasn't sure I wanted to share all
13 that information with the public.

14 (Laughter.)

15 But, as working utilities, we have a
16 major initiative towards making Illinois a smart
17 state, so it brings challenges for us and in defense
18 of each challenge Cloud components in this country.

19 MS. McKEON: Thank you all very much.

20 Each of you I think touched on
21 important information sharing in your opening
22 remarks, but I venture to say that most state and

1 public utility commissioners don't have security
2 clearance to get all of the information that perhaps
3 some of you can.

4 So how -- and, obviously, this
5 information is very sensitive. It shouldn't get in
6 the wrong hands, information about how these assets
7 are being protected needs to remain secure, but how
8 can regulators, such as our Commissioners, expect to
9 secure information, but also continue to monitor how
10 prepared utilities are at FERC for possible threats?

11 MR. LONBOM: I would like to comment on that, if
12 I could. I think there is a lot of work being done
13 to enable us to share the type of threat information
14 that Robert talked about, even if it's coming from
15 classified sources, and DHS is working with several
16 vendors, who's taking information about threatening
17 IP addresses and attackers that they're coming from
18 classified source that we're able to insulate the
19 classified aspect of it and deliver that service out
20 to about four or five specific vendors, so, from a
21 tactical perspective, we're able to share classified
22 information, if you will, at least to the point

1 where you can help protect yourself.

2 Moving up the information sharing
3 chain, we have a program within Illinois with our
4 Illinois Statewide Terrorist Intelligence Center
5 where we have a cyber program where cyber
6 information is pushed out to any members who wants
7 to subscribe to that. That includes government,
8 that includes police, that include private sector.

9 So, as a follow-up, if you are
10 interested, I can share some of the information that
11 you can get out to your members and folks in
12 Illinois who are interested in receiving that
13 information from a vendor to shadow that information
14 about the latest threats, so software
15 vulnerabilities, et cetera.

16 From a big picture perspective, the
17 challenges of CISO is to able to report to
18 non-technical boards of directors, commissions like
19 yourself, on whether we are doing a good job in
20 protecting our resources, so we have this challenge
21 in terms of how are we doing with our service. We
22 want to know what protection are you talking about.

1 We want to know how well we are doing and are we
2 improving.

3 I had the opportunity to meet with
4 several of the utility companies and partnerships in
5 very informal discussions about the protective
6 measures that they were putting into place, not
7 revealing any industry secrets by any means, but
8 what I was very encouraged is there is specific
9 frameworks that the utilities are following and
10 continue to follow.

11 We are here to talk about the NIST
12 cyber security framework, which is essentially an
13 English translation of the things we should be doing
14 to protect critical infrastructure, protect our
15 information, and I think there's other standards of
16 framework that Robert wants to speak about the
17 federal side that the utilities follow.

18 What I'm reporting to my board of
19 directors is our maturity about the cyber security
20 framework, a comprehensive view of all the things we
21 should be doing in cyber rated in an objective
22 manner that we can score against and see our

1 maturity increase.

2 If I was a board of director's member,
3 I would be asking MISO to show me your maturity
4 against the cyber security framework.

5 MR. IVANAUSKAS: I would add that if I were at
6 state agency right now, I would take a closer look,
7 of course, the local state Freedom of Information
8 Act statutes and then also the new cyber security
9 act. So under that act, certain information when
10 it's shared with the federal government and then if
11 the federal government shares it back to a state
12 agency, they're now just -- I'm testing my
13 memory -- so everyone's got to go check the law
14 itself, because I think there are protections from
15 the disclosure in the federal law on that
16 information that was given from a private company to
17 the federal government and then from the federal
18 government to the state of an immunity from being
19 required to disclose that under state law, and also
20 you want to check the recent fact (phonetic) act,
21 which is fixing the Surface Transportation Act of
22 2015, and that had a selection that modified the

1 Federal Power Act, Section 215.

2 Now Section 215 deals with the
3 mandatory standards of NERC. Now there's a new
4 Section of 215 (a), which the Department of Energy
5 and FERC are involved with and that does relate to
6 critical infrastructure information, especially
7 related to the electric power grid, and that statute
8 itself might also have certain protections on
9 information that goes to state agencies or local
10 governments as to whether any of that information
11 needs to be disclosed to the public, if a request is
12 under state law, or local law, or federal law.

13 So those are things to check. I'm
14 just going by my memory, but it's definitely worth
15 it. Also, long term those recent cyber security
16 act-type legislation at the federal level could
17 serve as a model for any state on how to best
18 balance the importance of Freedom of Information so
19 people -- so the taxpayer and the public can know
20 what their government is doing against the critical
21 need for a certain sensitive security information to
22 be protected because they were to disclose

1 throughout that there could be problems.

2 COMMISSIONER MAYE EDWARDS: If I can jump in, we
3 actually have -- I looked at that as well, so here
4 in the State of Illinois we actually don't have a
5 FOIA exemption, which is what you are referring to.

6 I know in Indiana they do, and that's
7 pretty recent. I know there are other states as
8 well that do it, but, what those state legislators
9 can do versus what we can do is really that comfort
10 level of getting the information right.

11 So what happens is when our utilities
12 are coming to us, and if they're sharing particular
13 information that they're giving to us, we almost
14 don't want it, because, okay, we are now -- we are
15 kind of a target. They don't want to give it to us
16 because it's kind of, okay, here's our master plan,
17 and I think it impedes their security obviously.

18 So one of the things I looked into a
19 couple of years ago was knowing about how we could
20 get a FOIA exemption. Of course, it's obviously a
21 long legislative process, but that is something I
22 think we -- I always have evaluated here, but,

1 unfortunately, we're not a state with that FOIA
2 exemption, and I think it works to our detriment
3 here in Illinois.

4 MS. HAURI: I think there's a way you can
5 collaborate within the confines. I'm still calling
6 it procedural. I always call them the confines, the
7 regulatory confines of communicating across
8 agencies.

9 Much of what I find is education and
10 awareness. It's a level-setting term, it's
11 understanding you're asking about a tabletop
12 exercise. That's a very valid question. It's
13 something we need to speak to we are or we aren't
14 doing this. We can understand what specific areas
15 you may have interest in, even work something like
16 that into it a tabletop exercise.

17 So I think open dialogue,
18 collaboration, communication, and openness to some
19 general education and awareness to the levels in
20 terms of what are those areas of concern. No, we
21 can't get into certain layers of our technology in
22 detail, because that's where the information is that

1 actually the bad guys would love to have, so that
2 can't be out in the general public, but the way
3 those systems and processes work and how they are
4 connected in more general terms those are definitely
5 conversations that I think we should be able to find
6 ways to communicate.

7 Again, we don't want to be giving
8 addresses, and the names of systems, and how they're
9 physically connected, where they're physically
10 connected, but, again, I believe that there are ways
11 we can collaborate, learn from one another, again,
12 understand what the concerns are, where they sit,
13 and where the system comes from to help us
14 understand that dialogue. I just think it needs to
15 happen more and it needs to happen.

16 COMMISSIONER ROSALES: As a Commission, I'm
17 looking for that checks and balances. I understand
18 Commissioner Edwards in terms of information that we
19 would receive.

20 One of the golden rules of business
21 for employees is they do what you inspect and not
22 what you expect, so how we review each of these

1 cyber security efforts makes a difference, and we
2 all know here at this table that we can't rely on,
3 well, it's been okay so far, so I know everything is
4 going well. That's -- we know that's a problem,
5 because when there is a problem, the problems are
6 usually pretty severe, so we are trying, as a
7 Commission, for that check and balance, but I think
8 utilities have been very good in allowing us to kind
9 of describe their cyber security efforts to keep us
10 abreast of the updates that they're working with,
11 but we also know that we can't just -- because
12 things are going well, we can't assume they're going
13 to continue to do well. That's something we can't
14 handle.

15 MR. LONBOM: That's a great point. The stats are
16 in some of our systems for 200-plus days before you
17 find out about it. We expect it's not about the
18 ability to compromise. We will be compromised and
19 the thing many of us worry about is how compromised
20 are we at any given time.

21 So I, too, totally agree with you. I
22 think the thought toward establishing frameworks

1 that a majority of issues against us is a nice
2 indicator for you to consider.

3 CHAIRMAN SHEAHAN: I have a question for Robert.
4 You know, we and other utility regulators around the
5 country struggle with the tension between being the
6 custodian to sensitive information and needing to
7 have comfort that the utilities are doing what they
8 should be doing, and I think you all mentioned this.

9 Are there other standards that we
10 could or should be requiring that the utilities
11 meet?

12 MR. IVANAUSKAS: There are so many different if
13 standards and categories. Is this one highly
14 respective?

15 The Department of Energy has put
16 together a set of -- I don't know if we can call
17 them standards, more of a framework for how to deal
18 with the issue. There's so many standards and
19 guidelines out there that there's not a single one
20 that you can recommend or endorse and say this is
21 the one.

22 Of course, there is the NERC cyber

1 security system, CIP standards, and those provide a
2 great baseline that have industry consensus, because
3 they come through the NERC process. Those will
4 apply to both power assets and there are different
5 considerations as there's different types of assets.

6 So you want to think long -- it
7 wouldn't be as simple as just a wholesale adoption
8 of the NERC standards for jurisdictional assets for
9 Illinois. So there have to be a lot of thinking
10 about that, perhaps even an industry
11 stakeholder-type process, plus there's the whole
12 question of jurisdiction that what is the
13 jurisdiction of the Illinois Commerce Commission to
14 act and what do you need to have done, and the power
15 act issues of jurisdiction over rates as compared to
16 jurisdiction over cyber security.

17 CHAIRMAN SHEAHAN: Well, I mean, the state
18 commissions certainly have responsibility for
19 reliability, and, you know, it's something we've
20 talked about at NARUC. It seems as though there
21 isn't really that -- you know, there is, you know,
22 the standard you talked about. There are, you know,

1 other standards. The White House has, you know, a
2 set of standards.

3 It may be a good opportunity for an
4 organization like NARUC to sit the state legislators
5 down and say, look, here are the specific issues
6 from a state level, not from a generation
7 necessarily. There are states that are restructured
8 like Illinois, but from a distribution standpoint,
9 as well as transmission, and here are some
10 additional standards that, through a stakeholder
11 process, we can all agree, you know, needs to be hit
12 rather than having the state sort of searching
13 around trying to figure out what standards we ought
14 to be holding the utilities to, which requires a lot
15 of expertise that we don't have necessarily that
16 requires being the custodian of a lot of data that
17 we don't really want to be custodians of
18 necessarily.

19 So it may be, you know, something that
20 NARUC, and FERC, other federal agencies could sit
21 down and kind of talk about coming up with kind of a
22 comprehensive set of standards that we could, you

1 know, all agree.

2 MS. McKEON: Tina, did you want to respond to any
3 of the comments made?

4 MS. HAURI: I would like to comment. Standards
5 are frameworks for us to work within.

6 I would say if all of our agencies
7 chose a standard and effectively implemented against
8 it to every person every day at a heighten
9 expectation level, we would all be in a far better
10 cyber control perspective.

11 I believe we are over-policied and
12 over-standard, because we are about 20 years into
13 cyber security as a discipline and practice across
14 business and government. I believe standards are
15 not our secret sauce.

16 I believe it's execution and the focus
17 and commitment to fulfilling the obligations that
18 those standards ask of us. Critical infrastructure
19 controls are in 28 control areas. Most groups are
20 probably doing well in three or four of them, which
21 means a whole lot of room for improvement for 17
22 more areas that we can all get better in.

1 So from a standards perspective, I
2 just challenge us to consider do we really need more
3 or should we choose one and work towards it and find
4 out what areas may not apply to the domain or
5 discipline and make exceptions for those but put a
6 longer eye focus on it. These will, again,
7 transcend administration, transcend election cycles.

8 Now some of the infrastructure is 20,
9 30, 40, 50, 90 years old, so we really do have to
10 take a long view and try to put in place something
11 that we can sustain against cyber security. It's
12 not going anywhere. It's here to stay with us.

13 Kirk, drew a line at the scale. I
14 draw the line at the refrigerator. My refrigerator
15 will not be speaking to me. It won't be telling me
16 I'm out of orange juice, but it will be connected.
17 Our homes are connected. Our cars are connected.
18 Our hips are connected.

19 I'm over in the DePaul building. If I
20 run into one more Pokemon Go person in my lobby,
21 because they're pretty focused on their phone and
22 stopping, we are disconnected.

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

(Laughter.)

We are going to work, play, commerce, through our work, we will be cyber connected.

So I think maybe we don't need another standard, maybe we just need to consider one and go for it and make it happen.

CHAIRMAN SHEAHAN: I wasn't suggesting we necessarily need to come up with an entirely new standard. There are writing standards out there, and from the perspective of a state regulator, you know, who's not an expert, it's tough to say -- you know, it's tough to answer the question are we really holding the utilities to, you know, the right standard.

MS. HAURI: Fair enough. And in this standard that Kirk has spoken to it does cross correlate or cross connect to some of the best known standards that are out there, whether it's the information security or the audit standards, but it is cross correlated. You can cross correlate, if you need to protect your credit card payments or health care data or the health care situation.

1 So I think we have been the
2 practitioner. We are actually hoping we get to a
3 fewer standard environment sooner than later, just
4 because it's very confusing and it takes a lot of
5 cycles of when the regulators come in to do the
6 assessment of our environment against our policies
7 and those standards.

8 It's cumbersome. It's laborious. It
9 takes days and days and days of our staff's time,
10 which means we aren't doing the proactive things we
11 likely be doing to better the environment, so
12 standard heavy or we can get so bogged down with
13 complying to our standards that we aren't doing the
14 right business.

15 MR. LONBOM: Just one more follow-up comment, but
16 I sort of have to add a little of my own admission
17 to try to promote the use of a cyber security
18 framework throughout the State of Illinois for a
19 couple of reasons.

20 One is developed in the federal level
21 essentially to protect the infrastructure. That's
22 what its focus was. When it was initially developed

1 it wasn't talk about government should adopt this in
2 the private sector. It's really about the critical
3 infrastructure.

4 I had enough an opportunity to talk to
5 some of the utilities during some sessions. We
6 found many of them written up in the cyber security
7 infrastructure.

8 I recently attended a conference in
9 Chicago made up strictly of private sector boards of
10 directors and members and the entire conference was
11 to help inform boards of directors' questions that
12 they should be asking in terms of asking their CISO
13 in determining if their infrastructures are being
14 cyber protected and in this cyber security framework
15 was the second portion of that conversation.

16 Again, I don't work to NIST. I'm not
17 saying it has to be the end all of all things. I
18 just think it's a great place to start, so I feel
19 very strongly about it over all the states.

20 COMMISSIONER McCABE: Robert, could you talk a
21 little more about the coordination at the federal
22 level. I know there's the Electric Sector

1 Coordinating Council. There's probably multiple
2 venues for the federal agencies to work with
3 utilities, transportation, RTOs, and others, on this
4 issue.

5 MR. IVANAUSKAS: You know, there are so many
6 different levels, and committees, and advisory
7 committees. I think -- I have a neighbor from the
8 National Government Association with a booklet that
9 sort of tries to list all of them, and I think they
10 have even missed -- I could give you the link. It's
11 in my bag here, but beyond -- I think the bigger
12 picture is the benefit that those collaborations
13 processes give.

14 So there's the reliability. There's
15 the trade regulations and making sure that the
16 auditing, the regulator is getting inside the
17 utility and seeing what's happening and making sure
18 that they're up to minimum standards, sort of
19 baseline standards.

20 On the other side, beyond that
21 baseline standard that everyone has to comply with
22 by law or by contract, there is the what are the

1 best practices, what's working, and what are those
2 threats out there. How do we -- If utility ABC is
3 having success in stopping a certain type of attack
4 or observes something that's unusual on their
5 system, there's got to be that system where utility
6 ABC can go to utility XYZ where even in the State of
7 Illinois, or through the federal government, or
8 through a committee of some sort, the SEC or DHS
9 committee, whatever committee, and they get that
10 information in the best practices out there.

11 NIST has committees. There's a
12 private organization called the National Electronic
13 Transmission Forum. They have collaborative
14 processes where they work together.

15 So there's the baseline issue of
16 trying to make sure that every utility is at minimum
17 standard and can meet it and it's testable or
18 auditable and it's met, and there could be reporting
19 obligations that if the utility itself sees that it
20 didn't meet a standard has to report that into the
21 state. There's that possibility, but then the other
22 possibility is let's look at ways to get best

1 practices, or what's working, or what's being
2 observed out there in a collaborative process where
3 people can talk.

4 Standards take a long, long time to
5 develop and think through and make sure that every
6 utility can comply with it and every state agency is
7 okay with being audited to it, and the threat
8 actors, the bad actors, they know that this is the
9 standard that everyone is messing with, let's do
10 something else, and the something else is what --
11 you've got to fix that something else through the
12 best practices, because if you can fix that in a
13 week instead of in a two-year process, then you can
14 stop those fast-moving threats, so this is a
15 two-part way of looking at it.

16 MS. McKEON: Any other questions from the
17 Commissioners?

18 COMMISSIONER MAYE EDWARDS: I do have a question.
19 Thank you very much.

20 I want to ask all of you, yet, and
21 answer specifically from the two people on the
22 panel, as you talk to about their interconnectivity,

1 so to speak, and I understand that as a CISO you
2 have to have an umbrella over your particular agency
3 in the state, or the city, but how connected are you
4 to the actual stakeholders in the city?

5 For example, if there were a cyber
6 attack -- and this is the question that we
7 oftentimes ask ourselves as well -- if there were a
8 cyber attack on one of the major utilities in the
9 city and the state, would you -- are you informed
10 about it? What is your role in it? Are you
11 involved in that process at all?

12 So I'm wondering interconnectivity
13 from that aspect, because, for example, a lot of
14 these targets we kind of speak of aren't necessarily
15 just the agencies but they're the major, you know,
16 businesses and organizations within a city or state
17 that can really attract that type of an attack.

18 Robert, I would love to hear your
19 thoughts on it as well.

20 MS. HAURI: You want to start from the state
21 level.

22 MR. LONBOM: Yes. I don't think we are as

1 connected as we could be. Obviously, there's a
2 concern about information sharing and, of course,
3 from private sector and things of that nature, we
4 have got those kind of things, too, stakeholders,
5 and things of that nature control information.

6 We do have a program that's the
7 Terrorism and Intelligence Center. We have good
8 communications so far with our infrastructure
9 partners where we do share information. We really
10 need to expand that capability and that
11 communication. I think it could be improved.

12 MS. HAURI: At the city level I have much the
13 same view over informal relationships that I need to
14 get after one on one to meet the people who are in
15 the key roles and even just to have the
16 collaboration and communication channel open.

17 We also have the Office of Emergency,
18 OET. They're quite connected. There's a weekly --
19 excuse me -- a bi-weekly meeting that we have of all
20 the public safety entities, so that's one way we
21 stay in touch, and that's my first link into the
22 connection that makes the city work, and, again, but

1 on a professional level I do have my to-dos is to
2 get out and meet my counterparts at the various
3 utilities and agencies who in the midst, if there
4 were a crisis, that would be my point of contact. I
5 don't want to have to find them when the crisis has
6 started. That's a bad plan.

7 So that is on my charter month to
8 month to start to reach out to the individual on an
9 informal level and figure out do we need to have
10 something more formal and what would that look like.

11 Back to the tabletop exercises, OEMC
12 does exercises. They take more of a public safety
13 view of things, but I think there's room for
14 collaboration and communication just like the state
15 has expressed.

16 COMMISSIONER MAYE EDWARDS: Thank you.

17 MR. IVANAUSKAS: I found my -- I went in my bag
18 and I got the Federal Cyber Security Programs
19 Resources Guide National Government Association, and
20 you take a look at it and there's a huge number of
21 programs, but this is dated October 2014, and I
22 think some of these programs might be sort of

1 phasing out, but the good -- and some of these
2 programs might still be in place. A state or a
3 utility might have contacted say DHS, for example,
4 or FERC and talked this through discovering that the
5 programs really wasn't working, and that was two
6 years ago, three years ago, and now the example of
7 DHS, the DHS program might be very far advanced,
8 completely different, a lot more functional, a lot
9 better, and it's constantly changing, evolving so
10 quickly, and that's a good thing, because we are
11 evolving quickly just like the threats are evolving.

12 On the idea that tabletop exercises
13 have -- of course, those are a great idea and, of
14 course, plans and being ready for resiliency, and
15 coordinating, and getting those communications
16 channel is critical.

17 The other critical part of that, of
18 the exercises and the planning, is to keep on doing
19 it, so every year NERC does this -- might be every
20 other year -- NERC has a big exercise drill where
21 they get top leaders in the utility industry
22 together to talk through and create these scenarios

1 of what might happen, and as the scenario gets worse
2 and worse, and it gets worse, the utilities, the
3 states, the federal government, and all of the
4 agencies and parts of it, see where the problems
5 develop. And when you identify where those problems
6 developed, then you fix them. Two years later you
7 have gotten through that state, but then you run the
8 test again and then at some point the system gets so
9 stressed that it again collapses. So the key is
10 just repeated testing, and planning, and practicing
11 over and over again.

12 MS. McKEON: Any other questions from the
13 Commissioners?

14 (No response.)

15 All right, we have got about four
16 minutes left, so I am going to ask that each of you
17 wrap up by letting us know what you think the number
18 one lesson that government actors should take away
19 from cyber attacks that have already happened, what
20 lesson is the biggest one.

21 MR. IVANAUSKAS: For me, and, of course, often as
22 I have been seeking for myself and my own opinion,

1 but for me the big lesson that I have learned is
2 that in a crisis, in an emergency, you'll be
3 surprised as to who is able to think most clearly
4 and act the most effectively, and for me maybe one
5 of keys is the people who practice the emergencies,
6 like the fireman or firewoman who practice those
7 emergencies and practices how to fight the fire,
8 well then when the real fire happens, it becomes
9 second nature and that's what really has to happen.
10 We have got to think through these things. What if
11 this happens to me tomorrow? What am I going to do?
12 Because when it does happen, and you create the
13 worst crisis that you can think of and go home
14 tonight and think it through, how am I going to deal
15 with it tomorrow, and then all of a sudden --
16 let's hope that it never does happen, but if it
17 does, you're ready. You're ready to act.

18 We have talked through a little bit of
19 your jurisdictional authority and what you are able
20 to do and what you can't. A lot of state utility
21 laws have sort of emergency powers that just aren't
22 exercised ever, if at all, and you've got to look at

1 those now, because you don't want to be looking at
2 them, opening that Public Utilities Act, at the last
3 minute saying what can I do? Am I really allowed to
4 do this? If I say this in public, what will happen
5 to me, and what will happen to the state, or how is
6 this going to work? That's my number one take away.

7 MR. LONBOM: I very much concur with that. My
8 history with Emergency Management continue to
9 especially look at nuclear plants and those
10 exercises that we continually find do very, very
11 well.

12 So I want to echo these remarks, and
13 as we are planning for state-wide cyber exercise in
14 the year 2017 or early 2018, we were very much
15 involved in the utilities and private sector with
16 that.

17 Just to follow up with that, I want
18 the opportunity to bring another on board which is
19 information sharing between public and private
20 partnerships. I mean, the pre-9-1-1 and type of
21 environment. We don't have that, but we need to
22 continue to explore that and move the barriers

1 between public and private sector and companies so
2 that we can have the appropriate level of
3 conversation to best protect the state and protect
4 the nation.

5 MS. HAURI: So preparation and collaboration are
6 key. Following on that is the number of scenarios
7 that you are prepared to deal with. It's different
8 each time. The kind of threats we face are going to
9 be cyber related, but cyber related has a number of
10 different subcategories that will come at us. Is it
11 going to be a website incident? Is it a ransom
12 incident? What kind of incident each requires a
13 slightly different kind of response.

14 So preparation is key, but preparation
15 down in a more granule layer is also key, because
16 that defines the scope and the scale of that
17 particular incident.

18 Also, your communication channels.
19 They have to be established internally across the
20 organization, as well as up, so that you understand
21 how the story is going to be told and how -- if it's
22 going to be an oppressed situation, who's going to

1 handle it and when are they handling it, and how
2 does that have to happen, and that has to be ready
3 24/7, 365.

4 So the threat is real. The scenarios
5 are real, the diversity of the threats are very real
6 and the response needs to be just as real and just
7 as ready.

8 MS. McKEON: Unless there are any other questions
9 at this time, please join me in thanking our
10 panelists for this great discussion.

11 (Applause.)

12 COMMISSIONER MAYE EDWARDS: Thank you so much.
13 Thank you so much, Robert, Kirk and Tina, for that
14 insightful and enlightening discussion and also many
15 thanks to our wonderful moderator, Anne. We will
16 now take a 10-minute break and resume promptly at
17 11:20. Thank you.

18 (Whereupon, a 10-minute
19 break was taken.)

20 Welcome back, everyone. If we could
21 have everyone take their seat, we will get started
22 with our second panel.

1 address cyber threats and how state public utility
2 commissions can play an active and purposeful role
3 in strengthening cyber security efforts,
4 particularly in the State of Illinois.

5 Joining me for this discussion are
6 representatives from RTO, as well the water, gas,
7 and electric utilities. So we have a nice variety
8 of perspectives on this panel.

9 Allow me to introduce Mr. William
10 Lucas, Director of IT Security and Compliance at
11 WE Energy; Mr. Nicholas Santillo, Vice President of
12 Internal Audit and Chief Security officer at
13 American Water; Mary Heger, Senior Vice President
14 and Chief Information Officer at Ameren; and
15 Mr. John Goode, Senior Vice President and Chief
16 Information Officer at MISO.

17 Please give our panelists a round of
18 applause.

19 (Applause.)

20 To begin, each panelist will present
21 from five to seven minutes giving an overview of
22 their company's efforts with respect to cyber

1 companies, both electric distribution, gas
2 distribution, transmission, as well as generation,
3 and we are in four states. In the State of Illinois
4 we have two gas companies that provide services. We
5 have a total service reach of 4.4 million customers.

6 Now there are some terms unique to the
7 utility industry. You heard some of these already
8 from our speakers earlier. I'm not going to read
9 through these. I will tell you to take a look
10 through. I apologize to you up front because I'll
11 be referring to these acronyms, like CIP, NERC,
12 FERC.

13 So what is SCADA, Supervisory Control
14 and Data Acquisition, for the utility industry?
15 It's very important. Basically what it boils down
16 to is any time we have a field or end-point device
17 and we want to communicate with it or extract data
18 from it, we need to do that over a communication
19 protocol circuit, if you will, back to our control
20 center. This is no different than other industries,
21 and we use it quite a bit as a utility for power
22 generation station control systems, substation

1 monitoring protection, electric distribution, and
2 transmission system monitoring and control, gas
3 distribution as an storage facility monitoring, as
4 well as on the customer side load generation usage
5 controls.

6 So what's the threat? You can
7 categorize cyber threats into four pockets, if you
8 will. We have the organized criminals. There's
9 somebody that is really out there to make money off
10 of your data, and they can do it. Obviously, they
11 to try to steal sensitive information if you will,
12 PII, credit card information or financial data.

13 Nation states that's usually a trade
14 secret kind of thing or maybe a state that's -- a
15 nation rather that is interested in something that
16 you are designing or developing, as a utility you
17 are designing. The tactic is more of an interest
18 from another country, maybe what we're doing if they
19 can get in or not.

20 Activists or social activism, we do
21 see some of that as a utility, and that's really
22 into groups that basically want to send a message.

1 They either don't agree with a stance or stand that
2 your business is taking, or something along those
3 lines, so we really look at things like business
4 disruptions, denial service attacks, website
5 defacement, and things like that.

6 The one that we're very concerned with
7 from a critical infrastructure perspective, and
8 that's terrorism, so that's kind of cuts down to the
9 core of state control, if you will. That's a lot of
10 folks.

11 The threats you have heard about, the
12 Ukrainian distribution grid blackouts tied back to
13 malware called Black Energy. Lansing Michigan
14 Board of Water and Light, they had some peak systems
15 that were shut down due to random attacks; Germany's
16 nuclear plant in Bavaria with malware attacks
17 compromising various log-in IDs, things are just
18 kind of across the board throughout all utilities,
19 if you will.

20 There's some concern about smart
21 grid and how those are attached to our control
22 networks, members is another point of entry from a

1 control perspective, DDOS, phishing attacks are on
2 the increase. You see a lot more of that, and then
3 programmable logic controllers and control system
4 vulnerability are also increasing. Those are also
5 increasing. That's mainly because those are spikes
6 are becoming more and more connected to computing
7 network, so be mindful of that.

8 I've skipped these two slides because
9 I talked about these. What we do and what we see is
10 kind of divided into categories. The first one is
11 risk governments. This is a big thing. It's really
12 important that you have the attention from the board
13 of directors on that, and by board of directors on
14 watch with respect to the importance of how you are
15 protecting especially critical infrastructure
16 systems and also what are you doing and how are you
17 doing it with respect to cyber, and that generates
18 your five-year plan and scope to how do we improve?
19 What are the most important projects from a risk
20 perspective to improve our enhanced security
21 posture.

22 That might go down to a steering

1 committee, so corporately that committee is chaired
2 by a CEO, and then also senior VPs of the companies
3 that you saw earlier.

4 So it's important that they understand
5 that, from a cyber security perspective, this is a
6 risk equation, a risk to the business, and it's an
7 understanding on their part or need to be an
8 understand on their part that if you are willing to
9 take a certain risk, these are the downsides to do
10 it if you do that.

11 There's very much interest in cyber
12 security attacks, what we need to protect, if you
13 will, at that level, and as well as at the board of
14 directors.

15 Information security steering
16 committee. So when you think about protecting
17 sensitive information, how do you do that? What's
18 important to the company when you know the business?
19 What is sensitive and how do you indicate that
20 through your employee base as well as how do you
21 protect it.

22 NIST CIP steering, so that's really a

1 committee of higher level management that really
2 crosses operation departments, as well as IT, and
3 that's really focusing on our control systems, so
4 critical infrastructure protection for the bulk
5 electric system and systems that are tied to that.
6 Sarbanes-Oxley, that's been a little bit longer.
7 Again, there's a whole cyber security that kind of
8 falls into that category.

9 Cyber security framework and maturity,
10 so we really focus on the NIST framework at WEC, and
11 in particular looking at the -- we actually perform
12 the Department of Energy Cyber Security Capability
13 Maturity Model, if you will, and we conducted that
14 for several areas, because the maturity level is
15 different between our control system network, if you
16 will, power plant network, and the like.

17 From that, we generated improvement
18 areas on that maturity scale, if you will, and
19 presented that to the ERSC and projectize a lot of
20 those improvements. That's an ongoing process.
21 It's done annually as far as reviewing where you are
22 with that maturity scale.

1 Incident response information
2 handling, we do share information on random attacks
3 with the electricity E-ISAC, AGA works (phonetic).
4 So not only do we get information from them on
5 attacks and certain and new events, if you will, we
6 also share back to them.

7 It's very important that we actually
8 keep those lines of communication open, and,
9 hopefully, we will get a better understanding of
10 what attacks look like. I call that actionable, so
11 we get actionable information to actually shut down
12 areas of attacks, if you will.

13 The FBI, DSH directors, we work with
14 those folks directly to help us further to better
15 define malware and we didn't understand what it's
16 doing, they are very helpful with respect to coming
17 in or reviewing code for us, a lot of help from
18 people both at the FBI and DHS.

19 Cyber security controls these are --
20 it's really like the basic bread-and-butter controls
21 -- excuse me -- so isolate corporate systems, access
22 management. I apologize.

1 Configuration management, that's
2 important, especially around the CIP access layered
3 security model, pretty much your standard
4 bread-and-butter security activity, protecting
5 sensitive information, policy and education for our
6 end users with respect to what is sensitive to the
7 corporation and how to protect it and share it, back
8 that up with data loss prevention tools and
9 encryption tools, as well as audit sensitive
10 information.

11 The third-party security support
12 services, we are no different than other companies.
13 We can't do it alone, so we do have services that
14 actually provide assistance to us with respect to
15 the denial certification.

16 End-user education and policy is
17 critical. Your end user is both your biggest asset
18 and probably your weakest link, so it's important
19 that you provide education, and it's annually,
20 monthly, do as much as you can.

21 Phishing is a big issue, training
22 folks in phishing we do that quite a bit. Look for

1 suspicious activity, acceptable use policies as
2 well, and then there's a list of sub-policies
3 underneath that that are across all companies, cyber
4 security, information security for protecting
5 sensitive information, as well as use of FOIA
6 exemption, as well as other policies.

7 MS. CROSSLEY: Thank you, Bill.

8 MR. SANTILLO: Okay. Good morning. My name is
9 Nick Santillo. I'm the Vice President of Internal
10 Audit and I'm also Chief Security Officer.

11 What's interesting is I listened to
12 Bill's presentation. I would say over 95 percent of
13 the items that were covered are consistent with the
14 way we operate.

15 So what I'm going to do I'm going to
16 focus a little bit on some of the areas so we are
17 not overlapping, but a little bit about American
18 Water. So we are the largest public-traded water
19 company in the United States. We have a diverse
20 footprint, so we are in 16 regulated states and we
21 cover all of our subsidiaries, all of our lines of
22 business. We cover about 47 states, so we have a

1 very diverse echo system of customers.

2 From a cyber security perspective, we
3 don't look at it as a subsidiary. We look at it
4 holistically. Our goal is to have a continuous
5 improvement across the security of all of our
6 footprint, so that's why I bring that up.

7 So as a regulated utility, we have to
8 balance safe, reliable water with just and
9 reasonable rates. Utilities do this, and cyber
10 security and security is part of that balance.

11 There's an additional balance though
12 that we do. It's a little bit like the Goldilocks
13 dilemma. Our goal is to find that security that's
14 just right. We don't want to not do enough security
15 because then we are investing in a security control
16 but maybe it's not fully mitigating risk.

17 We also don't want to have too much
18 security. There's a point of where you can have too
19 much security or you put too much investment into
20 areas there that would be better spent in other
21 areas, so the goal, as we look at it, is really to
22 find that just right security.

1 So a couple of questions. One of the
2 documents I provide as a reference is the Institute
3 of Internal Auditors, and ISACA put together a
4 document for boards. It's really about what are
5 those questions that the board should ask of their
6 management around their cyber security.

7 So I thought it was a relevant
8 discussion to look at how we approach the
9 Commission's cyber security, and the first question,
10 and we heard already a lot of discussion earlier, is
11 does the organization follow a security framework,
12 and that's a very important question.

13 At American Water we follow the cyber
14 security framework, you heard that mention. The
15 water sector has also adopted in this cyber security
16 framework for the sectors as a whole through the
17 water sector.

18 We sat down with the Water Sector
19 Coordinating Council of the EPA and DHS as well, and
20 we felt that the framework incorporated a number of
21 standards that sometimes utilities use in whole or
22 in part, so the framework approach we felt was very

1 good from being able to apply to all utilities, as
2 well as it gives enough flexibility for specific --
3 you know, for variations of specific controls, and I
4 think that's what makes it challenging when you talk
5 about standards, you talk about framework, is the
6 way that American Water may approach the security of
7 the system but it might be quite different than how
8 another utility may approach it, and that doesn't
9 mean it's right or wrong. It's just the idea is to
10 work within a framework so we have a consistent
11 approach, so we have adopted that framework.

12 The other question -- another question
13 to ask is what are the organizations' top five cyber
14 security risks? We feel that's a key question
15 continuously to ask. For us, we do a monthly
16 vulnerability review that we set up, and this is
17 your IT staff, a number of our IT managers through
18 our different disciplines and our security teams,
19 and we come together. We really look at what are
20 the merging trends, what are the current threats,
21 and how does that match against our footprint and
22 our control environment today, and what are those

1 top concerns.

2 We have a list of about 20 or so
3 sort of risk registered of those risks and monthly
4 we prioritize those. We always keep sort of to the
5 forefront what are those top concerns. I'll give you
6 a couple for reference.

7 So one of them is malicious malware,
8 for example, is a top concern for us, as well as,
9 you know, what we mentioned earlier, about Black
10 Energy and some of the malicious malware,
11 particularly targeting industrial control systems.

12 We do take that approach to isolate
13 those systems from our system, which is a very
14 consistent approach I think you will find with other
15 utilities, but we still keep that at the top of our
16 mind when we are putting our controls in. One thing
17 we will do is we will look at the vector that would
18 possibly be affected. Phishing is one of those top
19 concerns for us.

20 So we have actually partnered through
21 the Sanders Security Program is the one we selected,
22 and we actually go ahead and send every one of our

1 employees every month a phishing unit, and what we
2 do is we track the level of what we call
3 "quick-to-reality," and the goal is to drive that
4 down, because we recognize that's a top concern. It
5 also allows us to demonstrate some continuous
6 groupings in that space, so we've got a lot of value
7 out of that program. That's also one of the ways we
8 make cyber security known to all the employees.

9 A lot of times you think outside the
10 security and you think, well, that's just outside
11 the issue. It's really not. It's an every-employee
12 issue. It's one way we keep employees involved is
13 we have adequate security training and we roll it
14 out to all our employees, and that's really Cyber
15 Security 101.

16 We do the monthly phishing, which is
17 another way, and then we have targeted training for
18 more sensitive groups, such as HR, and we're focused
19 on protection of personal information.

20 We have within our data systems that
21 operate -- our data system while sectoring around
22 how to recognize indicators through the process

1 also, so we have these different target training
2 groups that we do continuously.

3 We do consider external and internal
4 threats. That's a key question that everyone should
5 ask is are you considering the internal threats as
6 well as external, and what we found is when we
7 started looking at this a lot of our controls were
8 geared around external threats, and we provide a lot
9 of access to internal employees, so we need to
10 control that address both external and internal
11 concerns.

12 And number five is about security
13 management and oversight, and I will kind of take
14 the last two together. With the way we handle
15 security over at American Water, as the chief
16 security officer, I work with the chief technology
17 officer and also our chief information officer, of
18 course, and that's our group. We present regularly
19 to our board of directors. We engage our Board of
20 Directors annually and we also conduct exercises
21 with our board of directors.

22 Last year we put together an exercise

1 series. We started with a technology exercise or a
2 more tactical exercise for IT, IT staff. We then
3 figured out how do I respond to the enterprises by
4 random incidents. We took that same exercise and
5 partnered with our insurance provider and said, if
6 this happened, what are those services we'll be
7 needing from you, and we did an exercise based on
8 that. We then took that exercise and we said, you
9 know, these are the operational decisions that are
10 being made. There's also leadership decisions that
11 have to be made around external notification,
12 communications, and then we did that same exercise
13 finally with our board of directors so the board of
14 directors could see sort of the results of the
15 entire chain of exercise. That was very successful
16 and then we are using that same philosophy.

17 What I think is the most critical on
18 this list is the last one, you know, we assume --
19 when we look at new controls and technologies or
20 evaluating new technology, we assume that that
21 technology is going to fail, so how do we respond,
22 and that's one way of approaching it. So I'll stop

1 there.

2 MS. CROSSLEY: Thank you.

3 Mary.

4 MS. HEGER: Good morning. I'm Mary Heger. I'm
5 Senior Vice President and CIO of Ameren. Ameren is
6 headquartered in St. Louis corporately but our
7 headquarters -- we also serve Ameren Illinois and
8 Ameren Missouri, those are our two operating
9 companies and we have an Ameren Transmission
10 Organization as well.

11 Our corporate IT organization provides
12 services for a shared service organization and we
13 provide services to the entire -- all of our
14 operating companies within Ameren.

15 In terms of our footprint, Ameren
16 Missouri is a traditional utility, electric utility.
17 We also have gas customers. We have generation,
18 and, as part of that integrated utility, we have a
19 nuclear plant, several coal plants, as well as
20 hydro-generation facilities, and in Ameren Illinois
21 we have our water and gas distribution facility.

22 The benefit that we have by serving

1 both Ameren Missouri and Ameren Illinois is that we
2 provide A critical infrastructure in terms of
3 nuclear coal, hydro, electric and gas, and we can
4 share those lines across our organization from a
5 corporate cyber team.

6 Ameren's mission is to follow the
7 quality of life, and we take pride in that from
8 across our entire organization and certainly our
9 cyber security program is no exception. We take
10 this very seriously and really spend a lot of effort
11 to make sure that we do provide safe and secure
12 energy to our consumers in both states, Missouri and
13 Illinois.

14 Our cyber security organization is
15 very similar to the ones that have been already
16 shown to you this morning, but I do want to
17 highlight a couple of things. Our board of
18 directors is very engaged with our program. They're
19 interested in our program. As a matter of fact, I
20 report to our Audit Group Committee each time they
21 meet in order to give them an update on our program
22 and the status of our program.

1 Our executive leadership team from our
2 CEO through all our operating company CEOs are also
3 engaged and informed about our program. Our IT
4 Steering Committee is made up of our officers across
5 the company who not only use our services from a
6 corporate IT perspective but also are responsible
7 for some of our control system, our SCADA, our ITS,
8 our generation control system, and we help set
9 policy and procedures as we move to a program along
10 with our IT steering committee, and then we have the
11 cyber security working group with managers and
12 directors from across the company that help us
13 implement and execute our program throughout the
14 organization.

15 Our cyber security team works daily
16 with our business segment in order to understand
17 what our policy needs to be and how we need to
18 implement that, and our program has varying
19 components that we review.

20 We have been, obviously, investing in
21 cyber security for many years, as have most, if not
22 all, of our peers. We do an annual assessment of

1 our program based on the current threat to the
2 landscape and we readjust our program where our
3 investment need to be made on an annual basis and
4 that is what is reported up through the chain in our
5 organization.

6 The other thing I wanted to mention is
7 you've heard many of these acronyms this morning,
8 and as we talked to our government and our partners
9 as well. One of the advantages that I found of the
10 utility industry is that we are very collaborative,
11 which is very different from many other competitive
12 industries, and I think, as a result of that, we
13 take that collaboration and that dialogue on for our
14 cyber security program and educated here by the
15 various partners that we work with both at the
16 federal and state level.

17 Critical infrastructure we take
18 extremely seriously. We are able to apply best
19 practices from across the various critical
20 infrastructure industries to other industries so
21 that we can really drive consistency across our
22 environment.

1 Our program obviously is to protect,
2 detect and respond. We have a multi-faceted best
3 practices strategy in order to do that and we
4 believe that we are continuing to mature our
5 capabilities day over day and year over year.

6 One other new program that we have
7 stood up Ameren in the past year or so is the crises
8 management team. Crisis management sits across the
9 organization and is accountable for really
10 responding to any type of a crisis that may impact
11 our business, be it a physical storm, a cyber event,
12 a physical event, pandemic, anything like that, and
13 we are very connected with them in terms of
14 communications, collaboration, and how we
15 communicate internally with Ameren, as well as with
16 our customers, and other business stakeholders and
17 partners, so that program has become very embedded
18 in the way we do business.

19 MR. GOODE: Good morning. I'm John Goode. I'm
20 the Chief Information Officer. Actually I should
21 turn my microphone on, shouldn't I. Off to a great
22 start.

1 John Goode, Chief Information Officer
2 at MISO, Mid-Continent Independent System Operator.
3 We manage the grid through our reliability services
4 in 15 states in the mid-continent region.

5 I would like to call it standing
6 manful (sic) in Mississippi and the gravy just rolls
7 off my tongue, which I enjoy.

8 We provide market services to 2000
9 generators with a variety of stakeholders, including
10 Ameren, a great partner on the panel.

11 In addition to that, you know, 80,000
12 miles of transmission line, peak generation, which I
13 think we are going to hit a new peak on Friday if
14 this weather continues, for about 127 gigawatts of
15 power.

16 Delighted to be here. I love having
17 the opportunity to come forward and talk about cyber
18 security and what our experiences have been, what
19 our lessons have learned, what we have learned in
20 the process, and also touch on where our failures
21 have been, right, so we can all learn from each
22 other and get to a more secured state faster and

1 hopefully keep the perpetrators at the door.

2 The slides I'm going to go through,
3 and I'm going to run through a couple of these, this
4 is the same information, this is the same slides
5 that we share with our employees, our management
6 team, our stakeholders, as well as our board of
7 directors, and these slides are set up to kind of
8 like generate an understanding of the problem at
9 hand, the comprehensive problem, and complex problem
10 at hand, as well as to raise awareness and
11 understanding of what we are doing on a daily,
12 weekly, monthly, yearly basis to make sure we are
13 not only protecting MISO but protecting the grid.

14 (Side presentation.)

15 Now if this will work.

16 (A brief pause.)

17 On this slide what I'm introducing
18 here is cyber is complex and it's increasingly
19 complex. We think about the technology industry
20 itself as one of the more rapidly changing
21 industries on the face of the planet, constant
22 invention, constant innovation going on.

1 Cyber is going even faster. The
2 perpetrators do not stop. They're relentless in
3 finding new vectors and avenues on attack to get
4 into our systems, so that leads us to believe that
5 it's almost impossible. There's no way you can
6 say -- your board looks at you and your CISO says we
7 are a hundred percent secure, they're not, so then
8 it comes to a balancing act of it's like what are
9 the appropriate risks that you are trying to
10 mitigate? What are the appropriate techniques and
11 capabilities you want to get out there to make sure
12 you can mitigate that risk where appropriate,
13 understanding who your perpetrators are, what
14 categories they're coming from, and it's a little
15 bit more than just stealing data when you start
16 talking about the companies that are involved here.

17 You know, you are on the grid. You
18 run nuclear plants. We run water over there. The
19 next 9-1-1 will probably be somewhat similar to
20 cyber 9-1-1, that being a physical attack. That's
21 something we need to prepare for.

22 When we start to think about it, it's

1 like my perpetrators, you know, some of them do I
2 need to protect against are the high school hacker,
3 the activist. The software nations say that. The
4 North Koreans are sitting in my system potentially
5 waiting for events, which they will rise up and
6 disrupt our economy and disrupt our capability by
7 shutting my systems down and potentially shutting
8 the grid down.

9 That's one of the things that we need
10 to be aware of that's a little bit different than
11 most cyber problems. That's not necessarily about
12 crime and data integrity. It's about disrupting the
13 American way of life in preparing for whatever will
14 come after that.

15 All right. And then the second slide
16 that we did provide in a snapshot really indicates
17 over the last five years I believe we have gone
18 through tipping point with the evolution of the dark
19 web and the cyber kit available to large quantities
20 of people about there, large numbers of people,
21 where you can basically go to school and learn how
22 to hack very easily, very simply.

1 We have seen the escalation with
2 malware. We've seen escalation with phishing.
3 We've seen the escalation with respect to the dark
4 web, yet, again, and it's real. Almost all the
5 companies you work for are having their network
6 perimeters probed on a daily basis, and whether
7 that's tens of thousands or millions of potential
8 hacks or probing, so those things are currently
9 happening.

10 So what we have decided then and the
11 approach that we have taken, that traditional
12 perimeter defense and strategy isn't good enough any
13 more. You need to build on top of it. You need to
14 build other capabilities, so the strategy that we
15 develop we call "intelligence-driven security."

16 And, we go the next slide, you can see
17 the components of this, right, the evolution over
18 time. There's still prevention. I'm still
19 investing in firewalls. I'm still investing in
20 defensive in-depth, and I'm still segregating my
21 infrastructure to make sure that as people come into
22 my infrastructure it's harder and harder for them to

1 move across it, right. You need to continue to
2 invest in that prevention, that defense in-depth
3 strategy and you need to increase your spend almost
4 year over year.

5 In addition to that though, what we
6 are finding out is that we really need to look at
7 having operational awareness around our network
8 activity. We need to know what the common patterns
9 are of our network, know the data, know the dynamics
10 of it, so we can look for minor anomalies, minor
11 trending in one direction that may lead us through a
12 program we call cyber hunting, the big bad guys
13 being in our network.

14 It requires big data analytics,
15 sometimes in real-time, sometimes close to
16 real-time. It requires a team of experts, and if I
17 look at the people that we have at MISO, Mark
18 Brooks, our Chief Security Officer, broad and deep
19 background within cyber, U.S. Army CISO, EMC, RSA,
20 Lilly, working in a variety of different industries
21 before we decided we needed expertise there; our
22 Mark Gable, our deputy CISO; Microsoft's star Buck

1 Roshien (phonetic), diagnostic CISO roles in all
2 those positions, and then, for example, Chat
3 Connell, who runs our cyber hunting team, Booz
4 Allen, numerous jobs with three letter intelligence
5 community companies, as well as being part of the
6 Air Force public security team.

7 Not only does it require the right
8 tools and techniques and the right processes around
9 it, you have got to look inside the vessel, triple
10 talent and then eventually the best internal
11 partners to work with, too, if you are going to be
12 secure.

13 A little bit more detail on our
14 intelligence-driven security strategy here, and just
15 a couple of points I want to make here, threat
16 intelligence. We spent a lot of time working with
17 the network, players throughout the industry, some
18 of our stakeholder players and their CISOs, what do
19 you see, what do you observe. That information goes
20 bidirectional. We also spend a lot of time with
21 vendors basically of getting reported on threat
22 activities that may be going on.

1 And, finally, I think one of the
2 things all of us mentioned, we have to a strong
3 instance response. It has to be drilled. It can't
4 be a dusty manual sitting on a shelf to pull out,
5 right. Your people need to know what to do, because
6 every attack is going to be different, and the key
7 here is the rapid response to that attack, again,
8 intelligence-driven security, of knowing what your
9 network is doing, to be able to identify it in
10 real-time and identify a problem, jump on it with
11 your instant response team and drive those guys out
12 before they create a problem for you.

13 The statistics will show that the
14 average advance persistent threat is 279 days from
15 breach to being found, and it's even longer for that
16 breach to be mitigated for those attackers to be
17 taken out.

18 One of the things that you will come
19 into as we talk with cyber, we talk about the fact
20 that it's impossible to be a hundred percent secure,
21 where do you know to make your investments, where do
22 you know to go, and risk management is a key portion

1 of that.

2 We have a fairly extensive risk
3 management program at MISO, too, and we use that to
4 evaluate our cyber security offerings. We have a
5 cyber advisory group -- a security advisory group,
6 right, which consists of business leaders at the
7 operational level. We track various metrics and
8 vectors within the security operating itself. We
9 report these frequently to our senior executive
10 team.

11 Our technology board has reports on a
12 quarterly basis almost, and each of these times
13 we're asking ourselves are we doing it enough? Are
14 we making the right metrics? Are we tracking the
15 right metrics? Are we making enough progress?

16 We using a standard set of frameworks
17 that we all talked about, MIS, EFC2, M2, and other
18 standard frameworks to be able to also monitor and
19 measure our progress against.

20 And then, finally, the last thing
21 within all this is just who are your partners. The
22 right people and having the proper intelligence

1 around cyber is extremely important, and, as we all
2 know, cyber security expertise is probably one of
3 the highest demand capabilities within the
4 technology community right now.

5 So we use a variety of partners, and I
6 think this is pretty much the whose whose on the
7 list of CISCO, McAfee, and others in the traditional
8 hardware partners, right, and then there's other
9 agency partners, Albanian, Grate-On, Instant
10 Response. They will drop a team in if you have a
11 problem, including cyber-corrective vendors, to
12 figure out who those bad guys are and what should we
13 do to get them out.

14 We use Solutionary and Lockheed Martin
15 for 24/7, 365 oversight monitoring of our cyber
16 capability. They're looking over the shoulder of my
17 own ITO, my own Innovation Technology Operating
18 sire, to make sure there are things that were not
19 missing, and Martin Lockheed-Solutionary can bring
20 in situational -- pardon me -- situational awareness
21 of what's happening not only in my industry, not
22 only within my system, but also nationally, as well

1 as globally from where the threat vectors are, and
2 probably they're increasing.

3 And, finally, we work with a variety
4 of other partners and players within the industry,
5 FBI, Department of Homeland Security, US-Cert,
6 Electricity ISAC, and then the RTO/ISO world in
7 general has a series of forums for CIOs and CISOs
8 also, exchange information on a variety of topics,
9 and, obviously, cyber security is extremely
10 important to that.

11 So all in all in closing, again, the
12 things we are most proud of is we take cyber
13 security very seriously, and we find that that
14 parameter defense in-depth traditional strategy that
15 we all had in place for the past 20 years are like a
16 starting point and we need to have that
17 intelligence-driven piece on it.

18 We really need to be cognizant of the
19 fact that we need to be constantly looking for
20 perpetrators in our network and not necessarily
21 having the hardware and software system with the
22 traditional protection finding it and finding these

1 guys.

2 MS. CROSSLEY: Thank you, John, and thank
3 everyone for providing an overview of your
4 companies' efforts with respect to cyber security.

5 If there are no additional questions
6 from the Commissioners, I would like to start by
7 touching on something that someone brought up in
8 your presentations and also something that was
9 brought up in the last panel that touched on how the
10 energy industry follows certain frameworks to ensure
11 adequate protections, particularly the NIST
12 framework, which I believe some of you have
13 mentioned.

14 The NIST framework is voluntary for
15 the energy industry to follow when implementing its
16 own cyber security measures, and since most states
17 currently do not mandate such measures, the energy
18 industry is self-regulating in this respect.

19 Is self-regulation effective or should
20 it be supplemented with some other formal government
21 action? Anyone?

22 MR. GOODE: I guess I'll go first and try to

1 answer that. One of the challenges -- I'm going to
2 divert us just a little bit, if you don't mind. So
3 one of the challenges that you have with any sort of
4 framework and any sort of standard for any sort of
5 regulation, it takes time to develop those
6 regulations, and frameworks, and standards.

7 So when you think about it, they're
8 always just a little bit out of date. So the way we
9 approach it, our adoption of this framework, and
10 EFC2, and MT, and other frameworks that we use to
11 try to make sure we have a basic set of cyber
12 security capability in place, so we can always look
13 to build on top of it, right.

14 So when I think about it, it's like if
15 we came in and created a new standard for the
16 electric industry or state-wide, that would probably
17 create more problems than it would hope to
18 accomplish because then you run the risk that every
19 state is slightly different, and a lot of us see a
20 variety of different partners and their partnership
21 opportunity may actually decrease making us less
22 secure, because now it's like if I operate in 14

1 states, I have 14 different state regulations to
2 follow when we're just following the federal. The
3 FERC and NERC regulations are difficult enough.

4 Does that give you a perspective?

5 MS. CROSSLEY: Yes, it does, but I know the
6 Chairman mentioned maybe it's not 14 different
7 states with 14 different standards, but maybe it's a
8 combination based on the NIST framework where you
9 all come together and come up with something that
10 you all could follow state to state. Is that
11 something --

12 MS. HEGER: I think, just to be clear, we talked
13 about this a couple of times this morning, but at
14 least in the electric sector, we all run mandatory
15 standards with regard to NERC, and many of us are
16 able to take those standards and apply those across
17 our environment -- in terms of best practices across
18 our environment.

19 Several of us are also nuclear
20 operators and there are required standards for
21 nuclear power plants to come out of the NRC, and,
22 frankly, with our nuclear standards and applying

1 those to other components of our infrastructure
2 where we felt that that was really a good best
3 practice.

4 In addition, most of -- -not all of us
5 have participated in the Cyber Security Maturity
6 Model c2n2, which was a voluntary program coming out
7 of the executive order, and we have been very active
8 in not only developing that model but in assessing
9 ourselves, and we use that model to really help us
10 determine where we're at in our maturity, where we
11 need to make our investments, and how we need to
12 mature our programs.

13 So I think, quite frankly, that model
14 gives us the agility and the ability to respond very
15 quickly as cyber security evolves and to really
16 mature ourselves and respond quickly where we may
17 have some gaps based on the current threats and
18 vulnerabilities of activities.

19 So at this point I believe that with
20 all of those things combined that we have sufficient
21 regulations and framework, and then, as we said,
22 it's not a one-size-fits-all for any of our

1 businesses, and we need the flexibility to respond
2 based on where we are currently at. Each
3 organization, even within our infrastructure, it
4 varies within a company where we are at, so how we
5 can response quickly and fill the gaps, in order to
6 protect this critical infrastructure. I believe the
7 framework in place to allow us to do that.

8 MR. SANTILLO: From the water sector perspective,
9 we did adopt the NIST security framework. The water
10 sector has also adopted that, so we feel it was
11 reasonable to adopt that framework.

12 AWWA, which is the American Water
13 Works Association, one of the primary standards in
14 the water sector, also developed a process by this
15 document based on this framework, and that's
16 really -- they actually took the framework with
17 respect to all sectors and actually pulled sections
18 out and provided almost a how-to guide on how to
19 implement that framework within the water sector, so
20 it really made it even more specific as we go
21 forward. So, as to the water sector level, that,
22 yes, is voluntary, but those are the activities at

1 that sector level.

2 MR. LUCAS: I'll just add that the DOE, the Cyber
3 Security Maturity Model, actually lines very well to
4 the NIST framework, so when you really go through
5 the maturity model work out when you've actually
6 achieving or looking at or addressing a lot of those
7 same security areas that NIST has out there, I'll
8 say the same thing for the CIP system -- CIP
9 standard. They actually do correspond very well
10 with the framework as well, maybe not all of them,
11 but they do correlate.

12 MS. CROSSLEY: Thank you.

13 Any questions from the Commissioners?

14 (No response.)

15 Okay. Well, it sounds like it's in
16 the best interest for your companies to invest in
17 your own assets, whether there's a voluntary
18 framework or a requirement.

19 One of the things you all mentioned
20 are how utilities are collaborating in partnerships.
21 So how are each of your companies working together
22 or how could you be working together more across

1 sectors to address cyber attacks?

2 MR. SANTILLO: I'll go first. So we participate
3 on a number of association-driven panels. So, for
4 example, ASI has a utility security council which is
5 a cross-sector council, so we actually have nuclear;
6 we have electric, gas, water; and this is a forum
7 where we can help both as a standard body driving
8 standards within best practices within the industry,
9 as well as collaborate across the members. We have
10 those same groups within our different associations.

11 So under the water sector we have more
12 than 50,000 water systems around the country, so
13 it's challenging, obviously, to get consistency when
14 we look across all of those water utilities.

15 So there's various associations, such
16 as the AWWA. On the private side, there's the
17 National Association of Water Companies. So where
18 those associations have set up groups and committees
19 around cyber security, we participate in those and
20 we need those, so those forums we found to be very
21 valuable and the cross-sector forums we also to be
22 very valuable.

1 On the electric side for electric
2 protection, there's EIS Council, Electric Security
3 Council, which is about protection of the grid, so
4 there's lots of standards, standard bodies out there
5 as well as forums for you to be engaged with, and we
6 find a lot of value in those. That's how we stay
7 sort of understanding what our peers and our
8 partners are doing and how we collaborate, as well
9 as with our federal partners as well.

10 MR. LUCAS: I'll add to that the EIS, the
11 Electric Institute, as well as the American Gas
12 Association. They have cyber security committees
13 that we are all members of and deal with. I'm on
14 the EEI of security for cyber mutual assistance
15 across utilities in case they haven't boots on the
16 ground, so to speak, so there's really good
17 collaboration around the utility industry.

18 MS. HEGER: If I could add a little bit more
19 detail around the Electric Sector Coordinating
20 Council, which has been mentioned this morning, but
21 this council is a council of about 30 CEOs across
22 investor-owned utilities from across municipalities,

1 and co-ops representing the entire North American
2 footprint of electric service providers, and this
3 group has been meeting now for several years and is
4 really intentionally looking at tools and technology
5 across the entire electric sector that can be used
6 to improve situational awareness. They're looking
7 at information sharing. They're also helping to
8 sponsor the cyber mutual assistance program that was
9 just mention.

10 So this team of really CEOs is
11 very highly focused on the criticality of what we do
12 and how interrelated our industry is, and I believe
13 that it has been recognized in terms of some of the
14 progress that we have made in coordinating with the
15 federal government and many of the agencies at the
16 federal level.

17 The recent GridEx Exercise that was
18 mentioned was performed in November. There were
19 over 400 entities participated in that exercise. It
20 was representing not only the U.S. but in Canada,
21 and in Mexico, and the CEOs of the ESCC met for a
22 situational awareness call as part of that, so we're

1 taking, obviously, incident response very seriously
2 through the GridEx exercise in how we collaborate
3 across the industry.

4 So, again, that's just a very real
5 example of the investment that the industry is
6 making in terms of collaborating across with our
7 peers and really driving our maturity across in
8 order to protect this critical service.

9 The other thing that should be noted
10 is they're also now beginning to reach out to other
11 critical industries that are important in the event
12 of some sort of an issue, so tell the communications
13 industry, the water industry, other industries, that
14 will have a likely impact, either on our ability to
15 provide services or that we would have an impact on
16 their ability to provide services, in the event of
17 an incident, so it's very active. It's part our
18 business right now.

19 MR. GOODE: I think I echo what many of our
20 esteemed colleagues already mentioned. There's a
21 high degree of collaboration within our industry,
22 the sharing of information around us, and I think

1 that's led in some measure to quite a bit of success
2 we have had with respect to cyber security.

3 The only thing that I would put out
4 there is potentially if speed of determining you
5 have a breach or what the latest threat vector is, I
6 think we could spend as an industry, and maybe just
7 the cyber technology in general, could spend some
8 time focusing on standardization or notification,
9 how do we get it to be system to system so we can
10 respond in sub-seconds to the next breach versus
11 what we are currently doing.

12 Again, I would like to also reiterate
13 I think we are in a really strong position. There's
14 always an opportunity for us to adjust a little bit.

15 MS. CROSSLEY: Thank you.

16 COMMISSIONER ROSALES: Nakhia.

17 MS. CROSSLEY: Yes, Commissioner.

18 COMMISSIONER ROSALES: A question for American
19 Water, perhaps we can do this off line, but I'm
20 interested in your goldilocks analogy, and my
21 question would be on the threat assessment graph
22 understanding there could be -- you could

1 over-invest; however, at what point -- at what point
2 do you draw that ceiling on your threat assessment,
3 if they have could get into your system but not
4 create a problem, is that okay or is a hundred
5 percent where -- at what point do you find the just
6 right level?

7 MR. SANTILLO: That's a good question. So the
8 attempt there is not -- and you highlight it really
9 about the risk assessment, and the key is, you know,
10 when we look at the risk assessment, we have a risk
11 and we want to drive that risk down, and you really
12 get into a risk appetite and work back up a little
13 bit, I don't think we can look at it as, you know,
14 we're not going to allow them to get in. Has it
15 ever occurred to you personally to learn about what
16 is our vulnerability.

17 So we really -- when we look at our
18 risk key map, we focus heavily on vulnerability,
19 because that's where it makes the most sense, and
20 the risk security measure or security control is
21 really about at what point have we driven that
22 vulnerability down to where it's maybe on the same

1 level as other risks that we have identified, so now
2 you have a consistent level of vulnerability.

3 So we really focus on initially sort
4 of at a high level of vulnerability. We want to
5 drive it down, but if we were to, for example, try
6 to continue to drive that vulnerability to zero,
7 we're not vulnerable at all.

8 When you get to a point of diminishing
9 return, it's not always very clear, and that's why
10 we take a collaborative approach. We do that with
11 all of our teams. We patch at this level. It's
12 going to take this much effort to go to the next
13 level. Do we want to do that and how much risk
14 reduction will we get?

15 So it's not an easy discussion, and
16 what we found the best way to do it is to do it as a
17 collaborative effort, because when we get all of
18 our, you know, technology together with the server
19 added there, right up to our CIO and CSOs on there,
20 we're able to really have a robust discussion, and
21 we found that to be the most effective.

22 Unfortunately, there's never that

1 perfectly right answer, and if we can't get it zero,
2 we want to make sure we allocate those risks. It's
3 definitely a balancing approach.

4 Does that answer your question?

5 COMMISSIONER ROSALES: Yes.

6 MS. CROSSLEY: Thank you.

7 We talked a little bit about
8 collaboration and information sharing before,
9 obviously, with information sharing there is some
10 risk to confidential information.

11 So what are the pros and cons in your
12 opinion of data and information sharing between
13 private sector critical infrastructure on its
14 operators and the government.

15 MR. SANTILLO: I'll take that one. So we do a
16 high level of information sharing, and we found out
17 that we share with commissions, as we share with
18 Homeland Security, and the FBI. There's actually
19 very little that we become very concerned with, and
20 we find that the discussions sort of around our
21 concerning areas aren't really relevant to the
22 information sharing anyway.

1 We are talking about the specific type
2 of control we have. When we talk about our
3 approaching, how are we protecting areas and types
4 of anomalies we are seeing, we feel very comfortable
5 sharing those at Commission level, as well with our
6 federal and our state partners, so we have not had,
7 I'll say, a big issue where we felt that we had an
8 inability to share.

9 MR. GOODE: There's a line to be drawn with the
10 information you can share, obviously, and we're not
11 going to share network diagram, and IPs, and ACLs,
12 and things like that, at a really deep level, just
13 generally talking about like what are the threat
14 vectors that exist, what do I need to do to look for
15 them. That's where most of the value is in
16 information sharing.

17 MS. HEGER: I would agree. I mean, we talked
18 about this, but in terms of information sharing, if
19 you think about personal privacy, we have found no
20 instances where personally identifiable information
21 has been a subject of information sharing that we
22 have with the government.

1 We are very encouraged and pleased
2 with the level of information sharing that is
3 currently occurring between the industry and our
4 governmental partners, and so we believe that it
5 needs to continue, and I think for obvious reasons
6 that we will all get stronger together and
7 information sharing is the foundation of that.

8 COMMISSIONER MAYE EDWARDS: I want to add -- go
9 ahead

10 MR. LUCAS: I was going to agree with what the
11 panel has said. We really haven't run into an issue
12 around information to government entities and
13 usually it's more of questions around the
14 technological side of things. Do we release a list
15 of our critical cyber assets? Well, normally that's
16 I guess against our policy to do that, but for a CIP
17 audit, we do. There's extenuating circumstances
18 that you allow that sort of thing.

19 I really don't get into PII, permanent
20 and identifiable information, or real deep
21 financials with those requests, so I think -- I
22 think it's important to collaborate. I really do.

1 You can do that to keep that type of information.

2 COMMISSIONER MAY EDWARDS: We talked earlier this
3 morning a little bit about for FOIA exemption. I
4 know we might be crossing over to the operational
5 side and none of you are actually, you know, general
6 counsel on that side of the house, let's say, but
7 do you have a different answer for those states
8 where there is a FOIA exemption? And I can explain
9 it more if you are not quite sure what that is.

10 Now I know Indiana, I know Missouri,
11 California, would you have a different answer where
12 there is a FOIA exemption and you don't have to
13 worry about any of that information actually being
14 FOIA or --

15 MR. SANTILLO: So we have -- we serve some states
16 that have that exemption and we serve some that
17 don't, and it's good to have it, because we can have
18 verbal conversations, but if we want to start
19 sharing written documentation, and, you know, if you
20 have requested, we will send it to you, we do have
21 to consider is that -- you have to put the lens on
22 it and say is this good public. We have to look at

1 what I'm going to send you is public.

2 If I know you can protect it, it's
3 just making that sharing with the commission side
4 easier and sort of, you know, we've removed any
5 barriers that are there. Yes.

6 Now we still share information
7 conversations, absolutely. Can we still work inside
8 those constructs? Yes, we can, but it does make it
9 easier when you have open dialogue than sharing
10 specifically written documents.

11 COMMISSIONER MAYE EDWARDS: You don't share as
12 much when there's no FOIA exemption?

13 MR. SANTILLO: I think it depends on the request.
14 I think there's definitely a thought process what's
15 being shared, so we have to share. There's
16 potential that we would be sharing less with a state
17 that doesn't have that exemption.

18 COMMISSIONER MAYE EDWARDS: Got you.

19 MS. CROSSLEY: We are running out of time, so I
20 would like to close with this question, and then
21 I'll turn it back over to the Commissioners for any
22 final questions or remarks.

1 Given everything that we have
2 discussed in this panel and the last, what do you
3 each consider the role of state public utility
4 commissions to be with respect to cyber security?

5 MR. LUCAS: For me, I just welcome the
6 collaborative sharing effort today. We continue
7 that dialogue will be great as far as I'm concern,
8 and then also we talked a little bit more and
9 discussed more about how we want to share
10 information with each other, because I think that's
11 important to talk about events that might be coming
12 up, and with respect to things that may impact the
13 State of Illinois, so let's continue our dialogue.

14 MR. SANTILLO: For me, I would say continuing to
15 collaborate I think as well as having the mechanisms
16 so we can continue to share information together.

17 The other area I'll say
18 interdependence. We talked a little about
19 interdependency between utility sectors and I think
20 the Commission is well positioned, whether it's
21 supporting an exercise or supporting those
22 partnerships or information sharing sort of being in

1 the lead seat for that.

2 I think there's opportunities there
3 for you to consider to really bring the utilities
4 together in a forum, and I think an exercise -- we
5 talked about an exercise -- tabletop and functional
6 exercise is one of the areas I think the Commission
7 is well positioned to do that.

8 MS. HEGER: Not to be repetitive, but I will be.
9 Certainly we do appreciate the dialogue that we have
10 had with the Commission over the years and I believe
11 the partnership that we have with the Commission,
12 and we really look to enhance that and to enable
13 more of those conversations, and I do agree that as
14 much as possible we can collaborate across the state
15 with other industries on how we can mature ourselves
16 across the State of Illinois, because we are so
17 independent, we are not in the State of Illinois, so
18 if there's some opportunity there, I think that
19 would be a good idea.

20 MR. GOODE: I think the collaboration has been
21 very well, very good, and benefitted both the state
22 as well as the industries represented here, and,

1 again, you know, with the typical John Goode
2 fashion, I will through out a little bit of a twist
3 on it, and, you know, I think there's one thing we
4 need to be conscious of the fact is that strong
5 cyber security requires significant investment in
6 both people process and technology.

7 If we could get to a point where there
8 were additional incentives on the investment side
9 for us to be able to continue those investments
10 without any budget pressure or any pressure
11 whatever, I think that would be a welcome area and
12 we can at least start to have a conversation
13 around it.

14 I guess the final piece of it is
15 we are really looking at that, plus the subject
16 matter with respect to cyber security, how do we
17 look at the next generation coming out of school and
18 set them to spend the time and get the degrees --
19 the advance degrees in cyber security so we have
20 this natural pipeline.

21 I think this is something that the
22 industry and state could collaborate on and you

1 could see some of the schools, like U of I and
2 others, continue to build on their effort in cyber
3 security and produce along the line of pipeline
4 cyber security professionals that we will be able to
5 produce in the future.

6 MS. CROSSLEY: Thank you very much.

7 Any final questions or remarks from
8 the Commissioners?

9 COMMISSIONER MAYE EDWARDS: I guess I have one
10 last question. You know, I think when I first
11 started kind of digging into cyber security, the one
12 thing I really noticed was there are a lot of
13 different authoritative agencies that kind of have a
14 hand in this, so the question is it FERC, there's
15 NERC that's involved, here comes the states, so,
16 obviously, it could be very frustrating not knowing
17 who your master, so to say.

18 Would you all prefer that there was a
19 strict delineation to say that we are going to
20 report to FERC on this, FERC is going to tell us,
21 you know, mandate our standards and the state is
22 kind of not be involved or do you welcome this

1 process when you can have almost eight different
2 hands in your cyber security pot, so to speak?

3 MR. GOODE: I'll go on this one. So we welcome
4 the conversation around cyber security. What are
5 the observations, the lessons learned, almost
6 anybody's willing to talk to us, because there's
7 always some other different perspectives we are
8 going to learn, we are going to get better from, so
9 I love having the opportunity to come here and talk
10 about this.

11 The other thing that we need to look
12 at then is this information sharing, and is this,
13 you know, us working together to make sure we are
14 pulling up minimal lowest common denominator when it
15 comes to cyber security or are we going to focus on
16 regulation and another audit, so we need to be
17 conscious of just what's the relationship, where's
18 the value added.

19 I'm regulated by FERC, I participate
20 in 15 states, Canadian -- I operate in 15 states,
21 the Canadian Province. I would be more than happy
22 to have you come in and learn what I'm doing, if

1 it's a very formalized audit, it's going to cost me
2 millions and millions of dollars to do that. I
3 would propose that that money would be better spent
4 on increasing my security posture versus getting an
5 audit again.

6 So I welcome the dialogue. Let's be
7 conscious of the value we're adding and that value
8 is bio-directional. We'll be learning at the same
9 time.

10 COMMISSIONER ROSALES: Nakhia, I want to make a
11 statement. I really appreciate the panels for being
12 here, and Commissioners Edwards, and the Chairman.

13 Historically, we don't have this type
14 of conversation until the catastrophe happens and
15 then we get together, so it's for us to be
16 proactive, this is what we have to do. We really
17 appreciate your being here and Commissioner Edwards
18 to put this together.

19 We are, as Commissioners, trying to be
20 proactive under the Chairman's guidance. This is
21 something we are trying to do and hope it's going to
22 work for all of us, because in the end, it works

1 very well for all of us here. Thank you.

2 MS. CROSSLEY: Thank you. On behalf of the ICC,
3 I would like to thank our panelists for taking the
4 time to be with us.

5 Please join me in thanking our
6 panelists.

7 (Applause.)

8 COMMISSIONER MAY EDWARDS: Thank you so much,
9 John, Mary, Nick, Bill, and Nakhia, for these great
10 and enlightening panels. It's really great to hear
11 from our utilities and our RTOs to consider
12 potential cyber threats and the efforts they take to
13 protect our critical assets.

14 With that, we will break for an hour
15 long lunch. Let's resume back here at 1:35. Enjoy
16 your lunch. Thank you.

17 (Whereupon, a lunch
18 break was taken.

19

20

21

22

1 COMMISSIONER EDWARDS: Good afternoon everyone,
2 welcome back from lunch.

3 Now that we've heard the security
4 perspective of stakeholders from both the public and
5 private sectors, I will lead the discussion amongst
6 industry experts about regulatory standards,
7 compliance, and best practices. Now, as you've seen
8 and heard throughout the day, cybersecurity is one
9 of the most urgent topics on the agenda for company
10 leaders and employees alike.

11 Attacks have been so common in recent
12 years, that the cybersecurity community has shifted
13 from a mindset of if we are hacked to when we are
14 hacked. The best prepared companies are shifting
15 their strategies from focusing on outright
16 prevention to implementing techniques to quickly
17 detect breaches.

18 This panel will discuss strategies and
19 best practices to provide guidance as we aim to
20 protect the nation's critical utility infrastructure
21 whole.

22 Now, our panelists for the session are

1 Jennifer Rathburn, partner and the co-chair of data
2 privacy and security team at Quarles & Brady; Bob
3 Lockhart, manager, cybersecurities programs with the
4 Utilities Telecom Council; Sharla Artz, director of
5 government affairs for Schweitzer Engineering
6 Laboratories Incorporated, the United States Energy
7 Association; and Annabelle Lee, principal technical
8 executive, cybersecurity power delivery and
9 utilization, Electric Power Research Institute.

10 Please give our panelists a great round
11 of applause.

12 Now, each of our panels will give a brief
13 presentation. Jennifer, feel free to begin when
14 you're ready.

15 MS. RATHBURN: Welcome, everyone. I'm going to
16 go over a little bit of what we've already talked
17 about this morning and really focus on the legal
18 aspects of what's going on in this space. It was
19 working a few moments ago.

20 I know we've discussed a lot about the
21 NIST cybersecurity framework and standards, but we
22 just want to give a little bit of a background for

1 all of the attendees. As you know, the NIST
2 framework, this is not a law. This is a framework.
3 It's not a regulation, but I can tell you that I
4 work in all different industries from finance to
5 healthcare, et cetera. And this is becoming the
6 best practice. NIST allows you to take whatever
7 industry you're in and really bring in those
8 regulatory standards of that industry.

9 And so I'm not going to go into detail,
10 but I wanted you to visually see how an organization
11 goes through the NIST cybersecurity framework. You
12 really have to figure out what is your business
13 context, where are you, where do I want to be. In
14 all areas you're not going to be perfect A plus.

15 But in certain areas, you do. And then
16 you have to assess where you currently are to kind
17 of figure out where you want to be and where your
18 analysis is. I think the NIST framework is an
19 amazing tool for government and/or organizations to
20 be able to figure out where to put your investment.

21 I know we've been talking throughout the
22 day, how do you solve the cybersecurity problem.

1 And really until you understand where you are and
2 where you want to be, you can't make good decisions
3 about where to invest money.

4 So we're not going to go over NERC.
5 We're going to talk a little bit though about some
6 of what became effective recently. These are
7 generally the NERC CIP standards for background
8 protection, which I'm sure you're well aware of the
9 standards.

10 But the reason the key changes that just
11 happens are related to really focusing on how to
12 deal with transient devices and removable media and
13 try to figure out the risks that are associated with
14 that. And when you're trying to figure that out
15 you're also thinking about your cyber systems and
16 cyber assets. And when you have high or medium risk
17 when you're trying to figure out how this
18 interrelates with removable media. So I just to
19 point that out that's something new.

20 The next issue is with regard to supply
21 chain management. We're going to talk a little bit
22 about that today. But in this most recent

1 Version 6, you know, FERC's order basically said we
2 want NERC to develop a supply chain management
3 standard. And today, FERC moved forward on that
4 final rule. We were just talking about this earlier
5 because they feel that it hasn't been flushed out
6 before it's a final rule. We want to give you an
7 update that that's moving forward.

8 One of the things as a lawyer that we
9 always looked at is where do the penalties come
10 from? What type of enforcement is out there. And,
11 you know, as you all know, that NERC conducts audits
12 on compliance standards and also violations can be
13 self-reported. We just want to point out that, you
14 know, penalties can be severe.

15 They be up to 1 million per incident.
16 That's generally not -- what we've seen is, you
17 know, \$1,000,000 fine per incident. But that is out
18 there and NERC has been active for many years. You
19 can see some of the, you know, some of the reports
20 showing how many violations.

21 But what I did want to talk about here is
22 some of the areas that they find most common are

1 really dealing with employees and workforce.
2 Training them, you can ensure that there's good risk
3 assessments about them. Good background checks,
4 making sure that employees have access only to
5 information that they need.

6 Also, you know, making sure if somebody
7 is terminated or moves on that they're, you know,
8 credentials et cetera are changed. There's also
9 been fines related to physical securities plans.
10 That's where some of the past enforcement actions
11 had focused. And we talked this morning, but I
12 think that that really allows, you know, government
13 or, you know, private companies to kind of get into
14 the minds of where America's focusing on.

15 So one other thing that I just mentioned
16 that under NERC CIP there is going to be a final
17 rule of supply chain guidance. In the interim there
18 is procurement language guidance recommendations
19 that are out there. And these are only some
20 highlights of the topics that are covered.

21 But obviously if you're purchasing
22 through the supply chain or you're in supply chain

1 this guidance is very informative. It's a few years
2 old, but at least it is a document out there in the
3 interim that does this provide some guidance.

4 I'm not going to go through these in
5 detail but here's just some examples of recommended
6 language you want to put in procurement contracts.
7 And this document is very detailed. And I do think
8 it's helpful. It is a few years old so some of it
9 is out of date. But it is a useful resource.

10 We talked about this morning about
11 information sharing. And I could not agree more
12 that this is entirely critical to developing a good
13 cybersecurity defense strategy. What is difficult
14 with cybersecurity is a lot of cyber incidents
15 happen to private companies that the government is
16 never aware of.

17 And I handle lots of cyber attacks. I
18 help companies prepare for them and respond and the
19 reluctance is to share information because they're
20 afraid of scrutiny whether from regulators or class
21 action suits. I think that information has been
22 really held close to the vest.

1 And so I can't agree more that
2 information really needs to be shared. Cyber
3 attacks, they change all the time. There's new
4 things coming into organizations no matter what
5 great policies or procedures you have, the cyber
6 attackers are way ahead of us.

7 Especially lawyers like myself feel
8 reluctant to turn over information about a potential
9 vulnerability that a company has experienced without
10 some sort of civil liability protection. So I think
11 this is going to continue to grow and grow in all
12 industries, and I think it's one of the best defense
13 mechanisms.

14 Before I finish up, because I only have a
15 few minutes, I know we're talking today about the
16 cybersecurity grid and reliability and cyber
17 concerns, but utilities also bring in information
18 related to consumers and perhaps credit cards, and
19 that information is well is sensitive and is
20 governed by Illinois State data breach laws and PCI
21 standards.

22 So that's also part of considerations

1 that utilities need to think about. I'm going to
2 turn over now.

3 MR. LOCKHART: Good afternoon, my name is Bob
4 Lockhart. I'm manager of cybersecurity programs at
5 UTC, which is the Utilities Telecom Council. First
6 of all, thank you for the opportunity to
7 participate. And really thank you for placing your
8 trust in UTC.

9 My role, I run the programs for
10 cybersecurity and also conversions at UTC. They're
11 both member driven programs so our member utilities
12 define most of the content in programs in what is a
13 key interest to them. And that enables them to
14 better execute in those areas.

15 UTC also has a substantial presence in
16 and telecommunications matters. Many of my comments
17 in response today are going to reflect what I
18 believe is best for utilities and for the customers.
19 As far as any requirements or rule that the
20 utilities focus on reliability or why utilities or
21 the regulators, personally, I spent six years as an
22 industry researcher working with utilities.

1 So after six years I still haven't found
2 a utilities that does not want to be secured.
3 Utilities really truly want to know answers to
4 questions, am I doing the right things. They don't
5 know. And they're looking for -- and they're
6 looking for help and looking for information.

7 The answers to those questions, though,
8 people want to compare their problems this morning,
9 you know, what kinds of people do you hire. There's
10 a lot of questions that utilities are trying to
11 answer, and they cannot do on their own.

12 One of the things UTC does is we provide
13 some peer to peer knowledge sharing and
14 communication platforms inside of our network. Some
15 of these are open -- they're all open to our
16 members. Some other to utilities and vendors.

17 It's kind of a safe place to discuss
18 things, and we've heard about fair sharing
19 information. We'll provide a place where utilities
20 can talk to each other and know that there's only
21 utilities online, and that enables them, again, to
22 share how to understand how to handle it.

1 You have to understand to really know
2 utility, you know. Is it a place where you're
3 likely to see a lot of clean energy technology like
4 rooftop or electric vehicles, how is the real energy
5 market structure? I live in Texas where we have
6 multilevel marketing selling of energy. Does.

7 The utility have a history of good
8 relationships with its customers? Those are just
9 attributes. If you take all presentation plus all
10 the other things you need to know to understand one
11 utility, it's really hard to come up with one set of
12 approaches that's going to fit all those different
13 utilities.

14 So from that perspective, we focus on as
15 we heard several times today, we like to focus on
16 outcomes. It's a little easier to generalize
17 outcomes than it is to generalize specific steps to
18 get to those outcomes. So it's my hope today that
19 my contributions to this session and those of all
20 the panelists up here will enable the State of
21 Illinois to create an environment where utilities
22 can thrive and provide a service the customers can

1 serve.

2 COMMISSIONER EDWARDS: Thank you.

3 MS. ARTZ: Thank you, Commissioner,
4 Commissioners, and Staff for including Schweitzer
5 Engineering Laboratories in the conversation today.
6 I had a former colleague who described cybersecurity
7 in the industrial control system as a three-legged
8 stool. If any one of the legs is missing, the stool
9 falls and we fail. These three legs are the private
10 sector asset owners, government, and it also
11 includes the manufacturers and suppliers of the
12 industrial control system equipment, which
13 unfortunately get left out of the conversation too
14 often. So I really appreciate being included today.

15 So let me explain who Schweitzer
16 Engineering Laboratories is so that you can
17 understand our role in keeping the stool upright.
18 About 32 years ago, Dr. Schweitzer invented the
19 first all-digital protective relay. This device
20 allowed utilities to identify faults on their system
21 without having to send crews looking for the fault.
22 And it also allowed utilities to restore power that

1 much more quickly.

2 Since that time, we have designed, built,
3 manufactured, and shipped products that touched
4 protection, control, automation, communication,
5 security, and metering in the electric utility
6 space.

7 We manufacture here in the United States
8 and Washington State and in Idaho. We actually have
9 a small facility in Lake Zurich, Illinois. So with
10 that being said, what we look to do is to -- as much
11 collaboration in this space is absolutely key. And
12 there are four main ways that SEL looks to
13 collaborate with our partners in government and in
14 industry to keep the stool upright.

15 The first way that we work on
16 collaboration is we keep security first and foremost
17 in our minds when we're designing and manufacturing
18 products. Dr. Schweitzer started his career at NSA,
19 so security has always been a big aspect of our
20 work. But we also listen to our customers on a
21 regular basis and try to understand what their
22 securities needs are. What kind of securities

1 functions and features are they looking for in the
2 products they're applying on their system.

3 Our engineers are training with the best
4 in terms of security practices, and they're also
5 thinking about ways to improve upon the security
6 features and functions in our products on a regular
7 basis. Quality is a huge component of the success
8 of our business. And one key component of quality
9 is the, you know, assurance that the materials that
10 you are putting into your product are doing what
11 they're supposed to be doing, that they're not
12 compromised.

13 So we have extensive practices and
14 procedures to help us mitigate the risk that's posed
15 by our supply chain and have been recognized. We
16 can go into more detail later in the Q and A, but
17 that is a very big part of what we do to ensure that
18 security is part of the products that we deliver.

19 The other way that we're collaborating is
20 we're working to understand the threat in the
21 environment that's out there. So we heard a lot of
22 discussion this morning about the first that

1 utilities are going to understand the threats that
2 they're facing. We do the same thing.

3 When DHS created the 16 critical
4 infrastructures membership in those sectors is
5 actually limited to the asset owners. So we will
6 get questions from our customers about what do you
7 know about this threat, and we would oftentimes have
8 to say we don't really know anything because we're
9 not privy to that information.

10 So SEL is part of the executive committee
11 of the critical manufacturing sector coordinating
12 council. And the main reason that we got involved
13 in this information is so we can understand the
14 threats that our customers are facing in the various
15 critical infrastructures, but also we could
16 understand the threats that are facing critical
17 manufacturers.

18 We also actively participate in efforts
19 linked with the critical manufacturing sectors such
20 as the recently formed DOE DHS supply chain working
21 group, which is working to develop the best
22 practices surrounding mitigating your risk from your

1 supply chain.

2 The third way in which we are
3 collaborating with our partners is we are
4 researching and developing new technologies to
5 address and improve cybersecurity and industrial
6 control systems. We were active participants in
7 both the initial development of the roadmaps to
8 secure energy delivery systems and then the update
9 to that road map.

10 And we are a recipient of grants from DOE
11 and their cybersecurity for energy delivery systems
12 program, which is a great partnership model of the
13 national labs, the utilities, and the suppliers
14 working together to come up with the technologies
15 that are going to address the gaps that were
16 identified in that road map.

17 And then the fourth way that we are
18 working to collaborate is in the development of the
19 best practices and the guidance that's out there.
20 We need to understand the regulations that our
21 customers are facing, the guidance they're using
22 such as the NIST cybersecurity framework, the

1 procurement language that they're coming to us with.

2 So what we're trying to do is get
3 involved in the development of these various
4 documents and initiatives so that we can bring the
5 supplier perspective to those documents but then
6 also understand the genesis behind what's being
7 proposed, what our customers are coming to us with
8 so that we can better meet the needs that they face.

9 So I'm going to stop there so we have
10 more time for Q and A, and I'll have more detail
11 when we get to that time.

12 MS. LEE: Okay. Thank you.

13 Thank you for the opportunity to talk
14 about what we do. I'm at the Electric Power
15 Research Institute. We are a not-for-profit
16 research organization that works with the energy
17 sector internationally, so we focus on research.

18 I want to step back just a little bit. I
19 know there are a number of utility people in the
20 room and talk about some of the differences and why
21 critical infrastructure and the operations
22 environment is a bit different from the IT

1 environment.

2 First off, if you look at the life cycle
3 of IT devices, everybody's got their phones and
4 laptops and so on. If you look at them, if it's
5 three years old, it's out of date. That's just the
6 reality. For the electric sector and this was
7 mentioned earlier devices may be out there 30, 40,
8 50 years. 50 years ago nobody worried about
9 security. I mean the focus was reliability. That's
10 still a focus.

11 And so how do you address cybersecurity
12 in an environment and a grid modernization where you
13 have the new devices, and I consider the
14 distribution component really the wild wild west of
15 modernization because that is where a lot of the new
16 devices if you look at renewables and so on, that is
17 the new area. Those are IT based.

18 You cannot run vulnerability scans on a
19 lot of these control systems. If you do, they shut
20 down. And if they shut down, people lose their
21 electricity. And on days like this people get very
22 annoyed if they lose their electricity.

1 Patches. And we talked about it and
2 you've seen patch Tuesday. In the OT environment,
3 patches are tested. They may be tested for six
4 months, they may be tested for two years. And then
5 you may decide that you're never going to deploy
6 that patch. That either the risk is too great or
7 the impact on performance is too significant.

8 So it's a very different environment.
9 And that's why again the whole infrastructure is
10 conservative. There are going to be attacks. I'm
11 just glad people say that. I tell people you are
12 going to get compromised. That's the reality of all
13 of our systems now. Focus on resilience. Okay?
14 Assume all of your systems have been compromised.
15 How do you keep functioning? You need to focus on
16 resilience.

17 You can't shut the systems down. Many
18 times you cannot isolate the device and say, Well,
19 we'll just isolate it or sandbox it and never worry
20 about it. You can't do that on control systems.
21 Again, you have impact on the overall functioning of
22 the grid.

1 You mentioned the different standards,
2 and I just want to give a little feedback. One of
3 the projects I'm working on on an advisory committee
4 for the European Commission. It's a government
5 thing. The name is God awful. We're looking --
6 it's Energy Experts Cybersecurity Platform Expert
7 Group. Horrible name.

8 And they are looking at guidance and
9 regulations for Europe. If you think our states are
10 bad, imagine getting all the EU members to agree on
11 what should be regulated or not. It's next to
12 impossible. They do look at the NERC CIPs. They
13 are looking that as guidance.

14 Mentioned earlier, the cybersecurity
15 capability, maturity model -- they are looking at
16 that. That's used. And another document is the
17 NIST report 7628, which is guidelines for smart grid
18 cybersecurity. That is also referenced throughout
19 the world. They're facing the same issues as
20 everybody else.

21 And if you look at from a vendor
22 perspective, vendors sell international. They don't

1 just sell to the U.S. or Asia. They have
2 international customers. So they want to develop
3 whatever tools and technologies that can be used
4 around the world.

5 Again, earlier, people mentioned as we
6 look at modernization and the inclusion of
7 information IT infrastructure and telecommunications
8 infrastructure in Washington, D.C., we learned a few
9 years ago a very high speed wind that comes down in
10 certain areas like a tornado, but lots of them.
11 That is when people realized you don't have water,
12 and you don't have gas. And I think Hurricane
13 Sandy.

14 So looking at the impact across all of
15 the critical infrastructures now is very important.
16 I'll just mention briefly that our role is a
17 research organization. We work with a number of
18 utilities as some of them represented here looking
19 at different areas. It's a matter of looking at
20 current threats and vulnerabilities. We're always
21 going to be behind. We have to be right
22 100 percent. Bad guys only have to be right once.

1 You know, that's the reality.

2 But figuring out ways of looking at
3 current threats, looking at future threats, figuring
4 out how do I add new terminology that's going to be
5 constantly changing and yet addressing legacy
6 devices. Some of those are still going to be out
7 there another 30, 40 years. The lead time can be a
8 year and a half, two years to get it. You're not
9 going to buy extra supplies and just have them
10 sitting around. But figuring out how to work in
11 this environment.

12 And if you want to know what the Number 1
13 cause of power failures in the U.S., and I'm sure
14 you know, it's squirrels. Number 2 is snakes,
15 particularly in the southwest, and I think Number 3
16 is birds. But it's squirrels.

17 COMMISSIONER EDWARDS: That was fantastic. Thank
18 you so much, all four of you.

19 So I kind of want to throw a question out
20 I think to all of you. Particularly the last
21 comments you talked about, the fact that it is here,
22 right? You're going to be compromised, deal with

1 it. And you talked in part to, you know, the
2 operating system. It's inevitable that this is
3 going to happen essentially.

4 So what ultimately would you say are the
5 best practices that we can put forward? And
6 something that comes to mind for me oftentimes a lot
7 of these incidents like you said we learn from past
8 mistakes and threats, oftentimes a lot of these
9 things and it goes to the -- it's kind of a hush
10 hush thing, right?

11 No one wants to talk about the exact
12 threats. There are some we knew -- last we heard
13 about what's going on with China with the FDIC, but
14 we don't know all the details. I was emailing you
15 very late last night because Southwest had some
16 system glitch that shut down literally the entire
17 website, their whole system. It's a little timely
18 for this system. But we'll never get the details.

19 So without getting all those details all
20 the time or most of the time and getting the nitty
21 gritty, how do we look at the past and look to the
22 future? What are the best practices when you

1 consider that?

2 MS. LEE: When I said that reliability is
3 Number 1 on the grid, that means that there's if
4 something happens, the first question is not, Gee,
5 is this a cyber incident? Guaranteed. The first
6 question of utility is okay, what device is down,
7 what system is down, how do we become operational.

8 So you may not know that was
9 cybersecurity and one of the documents that we have
10 produced when you talk about cases and failure
11 scenarios you can use for exercises, and the general
12 reaction has been total frustration from everybody
13 who's done it because they don't know whether it's
14 cyber or not.

15 Best practices, and I'd like the comments
16 earlier, that is up to each utility. In the U.S. as
17 was mentioned earlier there's incredible variability
18 in the size of utilities, the domains, whether
19 they're vertically integrated or distribution or
20 whatever.

21 You look at the large utilities. In the
22 southwest, the customers are a mile or two miles

1 apart, each utility has to make a decision. Again,
2 you can look at the documents to figure out where
3 you are in different areas. Each organization has
4 to make their own decision.

5 COMMISSIONER EDWARDS: Thank you.

6 MR. LOCKHART: I think a point we heard this
7 morning is don't wait to figure out what you're
8 going to do, right? So there's several faces to
9 that. The first one is executive level to
10 cybersecurity as an issue. I think somebody said to
11 that every month they send every new employee a new
12 phishing email.

13 And the other thing is the incident
14 response plan that was mentioned this morning as
15 well as having it ready. So there's a drill once a
16 year, twice a year.

17 MS. ARTZ: A couple of things. So DHS and the
18 FBI, a report earlier this morning this year, I
19 believe we can get links to that report. They did
20 an analysis of the numbers of data intrusions and
21 cyber attacks that they've witnessed and critical
22 infrastructure.

1 And 80 percent of those incidents would
2 have been through basic practices. So some of those
3 are not clicking on the phishing email, being
4 cognizant of the email that you're getting in, you
5 know, limiting privileges for your employees et
6 cetera.

7 So some of those very basic practices are
8 going to help us work a lot of these attacks. The
9 other aspect that I think we need to talk about when
10 it comes for best practices is knowing that we are
11 going to be attacked. It's looking very closely at
12 a recovery piece. And a basic component of that
13 piece and the utilities knows very well is the
14 fundamentals of electrical engineering.

15 So we not only need to train IT security
16 professionals, but we're also retiring a large
17 number of electrical engineers in this country. One
18 of the fastest areas that SEL was growing is
19 engineering services because utilities and another
20 infrastructure owners and operators are having
21 trouble having that talented workforce that's going
22 to be absolutely essential to keeping the lights up

1 when we do experience those attacks.

2 MS. RATHBURN: You know, we talked about our
3 tabletop exercises, but I wanted to explain how did
4 that evolve. You first think about what framework
5 are we going to adapt. So that's your bottom line.
6 You think about are we going to test ourselves
7 against that framework, are we going to bring in a
8 third party auditor? Most entities do that to just
9 do a background analysis or risk assessment.

10 Tabletop exercises are the next level of that, of
11 really doing that simulation, you know, in realtime.

12 And I have worked with various companies
13 on doing these, and I don't think there's any other
14 way how to prepare for a cyber attack or an incident
15 unless you do a tabletop exercise. Because when you
16 sit around the table with all the relevant parties,
17 and I would say perhaps supply chain as well, and
18 really think about, well, what if this got shut
19 down, what would we do. Would we be able to shut
20 that down?

21 And so I kind of want to explain it in
22 that way that's really like the new evolution of,

1 you know, doing a risk analysis. And it really is
2 like a risk analysis because you find the gaps.

3 COMMISSIONER EDWARDS: Kind of just for those of
4 us who aren't familiar with tabletop exercises --

5 MS. RATHBURN: Sure. I work with a company
6 called Delta Risk. They're a former Air Force.
7 It's a military term. It's practice, practice,
8 practice, practice. The military practices, you
9 know, for any sort of event. And so tabletop comes
10 from the military.

11 And really what it is you design mock
12 scenarios. And they don't even have to actually hit
13 your system. But, you know, there's preparation
14 usually an outside company sometimes they work with
15 me running through tabletop exercise, but it's
16 structured on the front end.

17 It's bringing in all of a company. And
18 I'm talking about IT, could be engineers, it's the
19 lawyers, it's the executives. And then you watch it
20 go realtime, and it's based on do you have an
21 incident response. You try to follow that, and I
22 can tell you that people think they have -- it

1 doesn't have to be incredibly detailed, but I deal
2 with a lot of cyber attacks.

3 They don't know what outside vendors to
4 use. And that's another thing. Not that the FBI
5 isn't helpful or other government agencies, but
6 oftentimes the real experts are actually in the
7 private industries.

8 So you have to hire those outside
9 forensic investigators or threat assessment. And so
10 you really need to sit and think. I think that
11 exercise allows an organization to really get a feel
12 of what would happen. You can't, you know, practice
13 for everything. But at least you understand how the
14 team works together and what you can and cannot shut
15 down.

16 COMMISSIONER EDWARDS: Fantastic.

17 MS. ARTZ: SO this was the first year that they
18 really tried to incorporate the suppliers into the
19 actual exercise, which was fantastic for suppliers
20 to think through how they're going to be responsive
21 to their customers. It's easy for us to respond and
22 say to one customer, but if it is a national level

1 incident, how are we going to support multiple
2 customers at the same time?

3 So having suppliers like us, GE, others
4 who were participating in this exercise, but prior
5 to this exercise, I know that utilities were
6 actually bringing some of their suppliers on-site
7 during the exercise to work through how that support
8 would work between the two entities. So that's an
9 important comment of the tabletop as well.

10 COMMISSIONER EDWARDS: So I agree with you on
11 that. One thing, I guess, voice that we don't hear
12 often at the table with this discussion is the
13 suppliers, the main factor. So now that we have
14 your voice here, why don't you walk us through,
15 paint the picture for us.

16 What, in that type of scenario, what is
17 your role? You know, just walk us through what a
18 day would be like in your shoes if something were to
19 actually happen.

20 MS. ARTZ: Well, you put me on the spot with a
21 really good question.

22 So our role is we actually have offices

1 all around the country and all around the world.
2 Because one of our goals is to be very close to our
3 customers to support their needs. Kind of
4 immediately, right? We want the lights to come on
5 as quickly as possible.

6 And oftentimes if there is any kind of
7 incident, it could be our devices that are in
8 question. So we have a support team that can get to
9 a customer's site within a couple of hours to help
10 them do assessments to help them do, say, forensics
11 analysis, reverse engineering on the product to help
12 determine if our products were involved or had some
13 help. And then we'll also work with our customers
14 to help them mitigate the event and to help them
15 basically get the system back up and running.

16 COMMISSIONER EDWARDS: So is it realistic to say
17 that -- well, let's say PG & E for example has a
18 huge cyber attack overnight, is it realistic to say
19 that in the midst of this chaos, so to speak,
20 they're going to call all their suppliers and have
21 you guys come on-site. Won't you kind of all be
22 walking over each other?

1 MS. ARTZ: Well, they will have identified
2 essentially their key suppliers, if you will. Who
3 they would contact first once they've done the
4 initial analysis of what is the potential root cause
5 of the event, right? And so also too because of the
6 NERC CIP requirement, right, a lot of those third
7 party vendors that have to go through training and
8 various background checks et cetera before we can
9 have access to their sites to do that analysis.

10 COMMISSIONER EDWARDS: Awesome. Well, that kind
11 of walks me into my next question. Are they, NERC
12 CIP and NIST, are they sufficient to protect
13 critical infrastructure from cyber attacks at this
14 point in time?

15 MR. LOCKHART: So first of all, again, nothing is
16 sufficient to just assume you're going to be
17 attacked. So there's a different between -- did you
18 say NIST?

19 COMMISSIONER EDWARDS: Yes.

20 MR. LOCKHART: So NIST is a framework, right?
21 And it really I hate to say this, it comes down to
22 the people because what we've seen in a lot of cases

1 with NERC CIP is, you know, security's really hard
2 and if you don't have any guidance and NERC CIP
3 looks like a recipe, and you just follow it and say
4 I'm good. You get focused on compliance that may or
5 may not be secure.

6 NIST is good because it's got a ton of
7 cross references. NIST requirement, here and maps
8 to this and so on. It's less about which one you
9 pick but that you pick one and do it and that you
10 understand. That's why I went through the laundry
11 list. So you got to understand what are all the
12 things I'm worried about, what are the risks, and
13 how do I address those.

14 MS. LEE: A few things, just comments. For the
15 electric sector, people have been talking data
16 breaches, IT deals with that typically and utility
17 organizations, IT has had to deal with data
18 compromises for decades and I agree. If they did a
19 lot of these compromises, if there had been basic
20 security controls, I remember the first thing about
21 15 years ago Bank of America, they have a facility
22 with multiple backup tapes.

1 Somebody broke in and walked away with
2 those tapes. The easiest thing to encrypt that
3 data. So looking at that, for the operation side of
4 utilities, and this is a bit of a generalization,
5 but the primary focus is availability and integrity.

6 You want to make sure that the systems
7 are available, and that the data that is sent is
8 correct. And that the commands that are received by
9 the various devices is correct. Confidentiality,
10 the protection of customer data is important. That
11 means when you look at a lot of these standards,
12 such as the number of the NIST series, they focus on
13 the IT side.

14 Those documents, those are guidelines.
15 They are not specific standards. Each utility still
16 has to make decisions about which of the controls
17 that are most important to them. And how they
18 should implement them. This is not, you know, a
19 laundry list.

20 NERC will very openly say the fact that
21 you can implement NERC CIPs does not mean that
22 you're secure. That's very much a baseline for the

1 power system. It's a start, but it does not address
2 all the cybersecurity issues.

3 So I can't give you a list and say you're
4 going to be in good shape. Each utility, they have
5 to do a risk assessment and prioritize the systems
6 and prioritize their controls. Small utilities,
7 they may not have anybody that knows anything about
8 cybersecurity. So they have to figure out what's
9 the best way of doing things when you talk about
10 tabletop and incident response. Some people have
11 literally have Excel spreadsheets or lists if you're
12 a small utility, that's all you need.

13 So there is no, again, no magic bullet,
14 no one list that fits everybody. Each utility has
15 to make sure their own decisions.

16 COMMISSIONER EDWARDS: Thank you.

17 So, Jennifer, we tend to say that systems
18 are only as secure as the people operating them.
19 Can you discuss the importance of training,
20 background checks, education, overall policies as it
21 relates to what I need to know.

22 MS. RATHBURN: Well, yes. For one, you should

1 only have people have access to what they need to
2 know. And that takes a lot of work on the front
3 end, that starts when somebody goes through
4 background check and HR process. But it also needs
5 to happen each time an employee or personnel changed
6 to a different job or when they're moved.

7 A lot of this has occurred because just
8 organizations have not kept up on that. It's also
9 an issue with insider threats and I don't think
10 there's really discussed today. But I co-founded
11 the Midwest Cybersecurity Alliance. They hold
12 meetings both in Wisconsin and St. Louis.
13 Background checks and making sure those people
14 really have access to what they need, also doing
15 data loss protection monitoring of systems.

16 But really, you can put all this fancy
17 technology into place, you can do assessments, you
18 can do tabletop exercises, but if you don't really
19 focus and bring cybersecurity at a cultural level
20 down to employees and not click on phishing and be
21 aware of their surroundings, I mean, you lose the
22 war.

1 I think what's really difficult about
2 cybersecurity I've been doing it awhile now, there's
3 no one size fits all. There's some best practices
4 that are out there and so it's frustrating because
5 it comes that three-legged stool, but it comes from
6 everywhere.

7 And so organizations really need to take
8 a multidisciplinary approach and that starts and the
9 employees understanding what the risks are. It's
10 teaching them about those risks.

11 MR. LOCKHART: You know, one of the threats that
12 wasn't mentioned on this morning was employee error.
13 You know, there's a technology aspect to the
14 protection that supports the people and you've gotta
15 process like work flows. But I think a security
16 awareness program, that is the biggest bang for your
17 buck.

18 Whether it's some people who do the class
19 once a year or someone do emails every week or all
20 kinds of different activities. But to get your
21 people aware, safety stuff, don't leave your laptop
22 in the car seat when you're traveling, stuff like

1 that.

2 Just getting your people to be thinking
3 about security I think there's very low technology
4 involved. So it's not the only -- but to me the
5 strongest part of it.

6 COMMISSIONER EDWARDS: Yeah. So I guess then the
7 next important thing is convergence, right? So
8 let's talk about that just a little bit.

9 When it comes to convergence, the word
10 utilities are lacking way behind. They have not
11 necessarily merged, IT and OT fluidly just yet. I
12 think more and more utilities are starting to do it
13 and are working on it. So can you provide any
14 suggestions for collaboration and coordination
15 between those two systems?

16 MR. LOCKHART: I think I mentioned IT and OT --
17 our members are all over the block. Some have done
18 a really good job. And the problem is there's too
19 much of an effort to solve this with technology and
20 as you mentioned, there's some huge cultural issue.

21 You have people from very different
22 backgrounds. People who got an degree in college

1 and other people who started their career with
2 climbing. We're seeing a lot of utilities where
3 you've got the same technology running in three or
4 four different departments being managed differently
5 by different people and there's no communication.

6 I've been in a meeting where the IT and
7 OT people started yelling at each other. And I
8 asked if I should leave the room and they said no.

9 One of our most successful members has
10 actually drawn up a document that all departments
11 involved agreed to and signed to. They've got a
12 page long made of up functions and who does what and
13 who's responsible. And to get everybody to agree,
14 we're all working for the same utility.

15 So it has to be a conscious effort to say
16 we all understand what we're doing and we're all
17 going to address it in writing very specifically.
18 Not just say, Hey we'd like to work together. So
19 the more structure you put on it.

20 MS. LEE: I'll jump on this one. When I talked
21 earlier about the integration, the IT and
22 telecommunications into the electric sector that

1 really forces this. As you said, a number of
2 utilities, a lot of utilities is are grappling with
3 this. The biggest issue we've done work on
4 utilities on this as a cultural side, how do you get
5 the communities together? And it's trust.

6 As I said earlier, the electric sector is
7 very conservative. You don't just change things.
8 You don't just modify. You don't just replace. The
9 OT devices are very sensitive. You put commands or
10 data in them. The typical response is to shut down.
11 IT has come in and run a vulnerability scan.

12 So it's a matter of the communities
13 getting together, understanding what each other
14 does. And how they work together and how they meet
15 their goals. They really are different communities.
16 Utilities and the ones that I've worked with, they
17 are getting together with the IT and the OT physical
18 isn't necessarily being integrated by -- if you want
19 to look at an incident.

20 Look at if somebody is in the substation
21 making changes if you have the physical access, are
22 they supposed to be there. Are they authorized to

1 be there. Do you know who they are. Do they have a
2 work order. Could be somebody forgot to sign in,
3 but if somebody is not supposed to be there and it's
4 integrated, all of that. But doing it from an --
5 I'll say from an OT side which is being more
6 conservative and more careful because of the
7 potential impact.

8 COMMISSIONER EDWARDS: Thank you.

9 Anybody have any questions at this point?

10 CHAIRMAN SHEAHAN: I'm kind of interested in your
11 thoughts on, you know, the idea that, you know, I
12 think we had a session earlier in the week and
13 someone thought, you know, threw out the idea that
14 there are going to be 50 billion sort of connected
15 points.

16 How do you know from a strategic
17 standpoint when you're thinking about every node and
18 in the grid, you know, potentially being a point of
19 vulnerability and home appliances and so forth, how
20 do you think about that from a big picture
21 standpoint?

22 MS. LEE: There was a discussion of defense and

1 approach, which is valid that comes from the
2 intelligence. But if you look at the electric
3 sector, because you have so many potential attack
4 points and attack surfaces, you have to look at all
5 of those points.

6 And I'm sure Jennifer knows this too.
7 Where that demarkation point is from the utility
8 perspective depends on which state you're in. Some
9 states, you know, their area of responsibility is at
10 the meter, some down in the devices into the home.
11 It depends on the state. It's not the same.

12 And also who owns your personal -- your
13 PII and your energy utilization. This is where, you
14 know -- and I mentioned earlier all of the new
15 devices -- it's sexy to have new devices. I don't
16 want to be walking around with a big, old laptop
17 that's ten years old that gets back to not only
18 utilities, but personal responsibilities.

19 Somebody else could hack into my phone
20 and see what's going on. So it isn't just the
21 responsibility, the utilities, or corporations, it's
22 individual responsibility to -- I saw a presentation

1 about ten years ago, and I couldn't think of any
2 tactful way of answering questions, so I kept my
3 mouth shut.

4 A city, they had a demonstration
5 where one individual was able to turn on and turn
6 off the streetlights from their phone. I couldn't
7 think of a way to say did you even think about
8 security? They thought it was neat. They could
9 drive around, turn on the streetlights and turn them
10 off. You've got to start thinking about the
11 consequences, and I think that isn't just utilities.
12 It's individual responsibility.

13 Doesn't help much, but I think, you know,
14 people have to start thinking what does this mean.
15 I can't just rely on somebody else to protect my
16 data, my systems. I have to think about do I really
17 want to do that, do I want to have all these
18 capabilities.

19 MS. RATHBURN: I'll just say a couple notes on
20 that is that I said that's where a lot of cyber
21 attacks and data breaches occur with new
22 technologies being added to a company. That's not

1 taking into consideration when somebody does a risk
2 assessment.

3 The risk assessment really is only good
4 on the day that you do it. So you have to
5 continuously reevaluate, to bring in this how does
6 that effect everything that we've done. And that's
7 complicated, and it's difficult. I think most of
8 the cyber attacks are implementing those new
9 technologies. In lots of other different spaces
10 after a breach is occurred and after doing an
11 analysis, it's really about did you consider that as
12 part of your risk assessment. Did you look at that.

13 And I think that type of approach from
14 regulators is really helpful to companies to
15 emphasize are you doing that risk assessment when
16 you're bringing in new technologies. That's just my
17 two cents from the breach perspective.

18 COMMISSIONER EDWARDS: What kinds of thing we
19 should be thinking about, very broad. Sharla, why
20 don't you switch it up just a little bit and talk
21 about supply chain considerations and why is that so
22 important when thinking about cybersecurity

1 measures.

2 MS. ARTZ: So Jenn mentioned the FERC, and then
3 the final order that was issued today because of
4 their concerns about potential malware to be
5 inserted onto devices, right, and then to be
6 deployed on the grid, and the threat that that
7 introduces then to the electric grid.

8 So as I mentioned before, for a lot of
9 suppliers, and when I'm talking about SEL, SEL as a
10 supplier, key trusted suppliers in this space are
11 going to be doing a lot of these same practices,
12 right? But we're going to be working -- quality is
13 essential to the success of our company, right, and
14 so if products don't do what they're supposed to do
15 or they misoperate, then that is not good.

16 So we work very hard in working with our
17 supply chain to make sure that we are delivering
18 quality products, and we do that a number of ways.
19 So this past year we had our 16th annual suppliers
20 conference where we brought in over 200 different
21 companies to sit down and explain to them what our
22 strategic needs are, what our security requirements

1 are, and just basically outlining the needs that we
2 have from that supply chain.

3 Our interaction with our suppliers is not
4 limited to that conference. We go out and conduct
5 regular audits of their -- are they following their
6 quality process, who are their Tier 1, Tier 2
7 vendors, right? So that we can learn about what
8 risks they might have from their suppliers.

9 The other thing that SEL does is we work
10 to vertically integrate, so we're trying to do as
11 much as we can inhouse, right. If we have to buy
12 materials, we have to outsource any parts of our
13 supply change. We write as much of our own code as
14 we possibly can.

15 And if we have to buy third party code,
16 we require that we have full access so we know
17 exactly what's in the code that has been supplied to
18 us. There's lots of ways that we check the way that
19 that code is -- that we check to make sure that code
20 is doing only what we are supposed to be doing.

21 So those are just a few examples of what
22 suppliers are doing. And we're doing this not only

1 because -- again, quality's essential, because our
2 customers are asking us questions, right. They
3 understand now that there is a threat posed, and
4 it's not new to them, right?

5 They are assessing the quality of the
6 products they're deploying on their system and have
7 been for decades, right. But they're asking the
8 really hard questions. It's essential for us to
9 rise up and meet those needs.

10 COMMISSIONER EDWARDS: Thanks so much.

11 As we wind down this discussion I want to
12 talk about just a couple of things. So we kind of
13 know obviously that utilities, there's a lot of
14 self-regulation, right? We talked about that a
15 little bit on one of the earlier panels.

16 And should utilities be incentivized at
17 all for security efforts or penalized for any
18 violations? What are your thoughts on that?

19 MS. RATHBURN: I can say definitely, I think
20 utilities should be incentivized for sure. And I
21 think that the Commission providing more education
22 and opportunities specific to help utilities with

1 regard to penalties. I mean, penalties only solve
2 one little issue. And it doesn't help the whole
3 process of cybersecurity.

4 MR. ARTZ: I think one of the ways that the
5 industry can be recognized is -- and Robert from
6 FERC mentioned this -- alluded to this earlier
7 today. When I was doing cybersecurity and
8 industrial control systems at Schweitzer, this is
9 probably back in 2009, 2010, there were 27 active
10 working groups trying to address industrial control
11 systems cybersecurity, right. What do utilities
12 need to be doing, right? And they needed technical
13 experts that were not just technical expertise and
14 electrical engineering.

15 As we discussed that's a limited pool of
16 people that need to be doing their day jobs every
17 day, just keeping the lights on and WARGD off
18 attacks. So I think what I have seen a number of
19 years the electric utilities providing those
20 resources to those various government entities
21 whether they be at the state level or the federal
22 level trying to be active parts in that space and to

1 recognize a tremendous amount of effort that they
2 have done to improve here.

3 Because I think too often they get a
4 lot -- for not doing enough or not participating
5 whatever working group it is. And so I would just
6 essay recognizing the tremendous amount of effort
7 that electric utilities have done in this space.

8 COMMISSIONER EDWARDS: So kind of on that same
9 vein, how can we encourage you to at least be more
10 transparent with us and to have more open
11 communication with regard to cybersecurity?

12 MR. LOCKHART: That's usually when there's a
13 two-way benefit, right? I mean that's when the
14 communication happens. I don't know what the ICC
15 jurisdiction is, but when we talk about the large
16 groups, they have a lot of resources, right? The
17 ability to figure out just about anything and solve
18 just about any problem and apply lots of resources
19 and manpower to it.

20 But there's so many in this state here,
21 that they just don't have the ability -- you know,
22 to put those kinds of resources, so they have to

1 have somebody to talk to. It's not only the major
2 utilities you want to hear from.

3 COMMISSIONER EDWARDS: Well. Hopefully our
4 utilities know that we want them to win. Hopefully
5 they'll be transparent with us when necessary.

6 I want to open up the floor again with my
7 colleagues before we wrap up this panel.

8 CHAIRMAN SHEAHAN: I just wanted to thank you,
9 Commissioner Edwards, for pulling this together and
10 all the guests have really been a terrific panel.

11 COMMISSIONER EDWARDS: Thank you, I appreciate
12 that. That concludes our discussion. On behalf of
13 the Illinois Commerce Commission, I'd like to thank
14 our panelists today to explore this topic with us.
15 Please join in on giving them a round of applause.

16 I also want to offer one last thanks to
17 all of our panelists for their participation. We've
18 learned a great deal thanks to everyone's expertise
19 and willingness to engage in an open discussion. As
20 the Chairman mentioned, we will not stop here. We
21 will keep moving forward and keep pressing forward
22 and use all of you as a great resource.

1 I certainly want to thank my legal and
2 policy advisors, Annie McKean and Nakhia Crossley.
3 They did a wonderful job moderating the discussion.
4 I'm extremely proud on many levels.

5 With that, this meeting is adjourned.

6 Thank you.

7 (Whereupon, the proceedings ended
8 at 2:47 p.m.)

9
10
11
12
13
14
15
16
17
18
19
20
21
22