

1 FERC/DOE Security Investments for
2 Energy Infrastructure

3

4 Technical Conference

5 Docket No. AD19-12-000

6

7 Thursday, March 28, 2019

8

9 Federal Energy Regulatory Commission

10 888 1st Street, N.E. Room 2C

11 Washington, DC 20426

12

13 10:00 a.m. - 4:00 p.m.

14

15

16

17

18

19

20

21

22

23

24

25

1 SPEAKER LIST
2 Bruce Walker
3 David Pekoske
4 Chairman Neil Chatterjee
5 Commissioner Cheryl LaFleur
6 Commissioner Richard Glick
7 Commissioner Bernard McNamee
8 Joseph McClelland
9 William Evanina
10 Chuck Kosak
11 Sonya Proctor
12 Nicholas Akins
13 Mark Gabriel
14 James Robb
15 Thomas Galloway
16 Donald Santa
17 Christopher Crane
18 Nicholas A. Brown
19 Jay Scott Emler
20 Kevin G. Wailes
21 Paul Kjellander
22 Alan S. Armstrong
23 Upendra J. Chivukula
24
25

1 Panel I Panelists:

2 William R. Evanina, Director, Office of the Director of
3 National Intelligence, National Counterintelligence and
4 Security Center

5 Robert Kolasky, Director, Department of Homeland Security,
6 Cybersecurity and Infrastructure Security Agency, National
7 Risk Management Center

8 Charles P. Kosak, Deputy Assistant Secretary, Department of
9 Defense, Defense Continuity and Mission Assurance

10 Sonya T. Proctor, Assistant Administrator of Surface
11 Operations, Department of Homeland Security, Transportation
12 Security Administration, Security Operations

13 Nicholas K. Akins, President and CEO, American Electric
14 Power

15 Mark A. Gabriel, Administrator and CEO, Western Area Power
16 Administration

17 James B. Robb, President and CEO, North American Electric
18 Reliability Corporation

19

20

21

22

23

24

25

1 Panel II Panelists:

2 Christopher M. Crane, President and CEO, Exelon Corporation

3 Nicholas A. Brown, President and CEO, Southwest Power Pool,

4 Inc.

5 Jay Scott Emler, Commissioner, Kansas Corporation Commission

6 Kevin G. Wailes, CEO, Lincoln electric System and Co-Chair,

7 Electricity Subsector Coordinating Council

8 Paul Kjellander, Commissioner, Idaho Public Utilities

9 Commission

10 Alan S. Armstrong, President and CEO, Williams

11 Upendra J. Chivukula, Commissioner, New Jersey Board of

12 Public Utilities

13

14

15

16

17

18

19

20

21

22

23

24

25

| | TABLE OF CONTENTS | |
|----|---|------|
| | | PAGE |
| 1 | | |
| 2 | | |
| 3 | Opening Remarks and Introductions | 6 |
| 4 | Panel I: Cyber and Physical Security, Best | |
| 5 | Practices, and Industry and Government | |
| 6 | Engagement | 32 |
| 7 | Panel II: Incentives and Cost Recovery for Security | |
| 8 | Investments | |
| 9 | Closing Remarks | 206 |
| 10 | | |
| 11 | | |
| 12 | | |
| 13 | | |
| 14 | | |
| 15 | | |
| 16 | | |
| 17 | | |
| 18 | | |
| 19 | | |
| 20 | | |
| 21 | | |
| 22 | | |
| 23 | | |
| 24 | | |
| 25 | | |

1 P R O C E E D I N G S

2 Opening Remarks and Introductions

3 CHAIRMAN CHATTERJEE: Good morning everybody and
4 welcome to today's Technical Conference hosted jointly by
5 the Federal Energy Regulatory Commission and the Department
6 of Energy to examine security investments for energy
7 infrastructure.

8 I'm so pleased to see such a robust audience
9 today. I'm told this is the largest audience in response
10 that we've had to a FERC Technical Conference, and
11 considering the fact that today is not just opening day, but
12 Zion Williamson practice day in D.C., I am very pleased to
13 see this turnout.

14 I'm also very pleased to welcome our cohost from
15 the Department of Energy, Assistant Secretary Bruce Walker
16 and Principal Deputy Assistant Secretary, Patricia Hoffman.
17 I'd like to also thank our distinguished guests from the
18 Transportation Security Administration, Administrator David
19 Pekoske, thank you so much for being here.

20 I'd also like to welcome our expert panelists
21 representing a broad spectrum of the energy sector, thank
22 you all for your participation.

23 I've talked many times about the exciting and
24 transformational benefits of innovation we are seeing in our
25 current energy landscape. But we have to remain mindful

1 that as technological advancements transform the energy
2 sector, and increase opportunities for consumers, the
3 threats that we face also are transforming and increasing.

4 This is particular true when it comes to cyber
5 security vulnerabilities. Unfortunately, the threat of
6 malicious actors targeting our nation's critical
7 infrastructure is part of the new reality we have to contend
8 with, which is why I think today's conversation is both
9 critical and timely.

10 Before I speak to some of the things I'm hoping
11 to accomplish today, I'd like to take a moment to recognize
12 the significance of the group that we've brought together.
13 Sitting around this table we'll have leaders from a variety
14 of government agencies or regulatory bodies, that have a
15 shared responsibility for the security of our energy
16 infrastructure.

17 That includes FERC, DOE, NERC, TSA, ODNI, DHS,
18 DOD, and of course, our state partners. On top of that
19 we've got some extremely impressive representation from the
20 private sector and public power. Everyone has an important
21 role to play in securing our nation's electric and pipeline
22 infrastructure, so I'm looking forward to listening and
23 learning from one another and finding ways to work more
24 effectively together, moving forward.

25 On this point, I'd like to recognize our special

1 guest, TSA Administrator David Pekoske. I recently met with
2 the Administrator to discuss pipeline, cyber and physical
3 security. I was impressed by his focus on this vital issue,
4 as well as his plans to strengthen TSA's program in this
5 area.

6 As part of these ongoing efforts, TSA has been
7 working collaboratively with FERC and DOE through the DHS
8 National Risk Management Center, to conduct in-depth cyber
9 security reviews with pipeline companies during fiscal year
10 2019.

11 I appreciate the Administrator taking the time to
12 join us for today's Techno-Conference, and that a key member
13 of his team, Assistant Administrator Sonya Proctor, will be
14 participating as a panelist in our first session.

15 So, now that we've assembled this impressive
16 group where do we go from here? As I've noted previously,
17 here at the Commission we are continuing to look at the
18 larger issues of resilience, but I think this Technical
19 Conference is an important opportunity to take a targeted
20 look at the issues of investment in cyber and physical
21 security.

22 So, with respect to the first panel, my goal is
23 to better understand the need for security investments that
24 go beyond those measures already required by mandatory
25 reliability standards. While we need to think creatively

1 about how to address cyber and physical threats, I recognize
2 that it is not possible or cost effective to design our
3 energy infrastructures to withstand every type of attack
4 that could possibly occur.

5 Striking the right balance for consumers is a
6 complex, but important undertaking. To that end, I hope to
7 examine where we should be focusing our limited resources.
8 For the second panel my goal is to better understand the
9 factors that can hinder or help when it comes to making
10 security investments.

11 Specifically, I'd like to hear about any barriers
12 to recovering the costs of security investments at either
13 the state or federal level. And even, if there are no
14 barriers, I'd like to hear suggestions for things this
15 Commission could do, to further incent utilities to go above
16 and beyond the minimal requirements of the reliability
17 standards for the benefit of consumers.

18 The issue of incentives for transmission security
19 was also teed up in the notice of inquiry on transmission
20 incentives we issued last week. So, our consideration of
21 this topic won't end with our conversation today.

22 With that, I'd like to turn the Technical
23 Conference over to Assistant Secretary Bruce Walker for his
24 opening remarks.

25 MR. WALKER: Thank you Chairman. I would like to

1 sincerely thank Chairman Chatterjee, each of the
2 Commissioners, and all the panelists that are here today to
3 testify on a significant national security risk -- the
4 threat to our infrastructure.

5 Many, if not most of us in this room today
6 witnessed the fall of the Berlin Wall on November 9th, 1989
7 and the end of the Cold War. Those were remarkable events.
8 With these events, the fear of nuclear war was greatly
9 diminished. Complacent in our victory in achieving world
10 dominance through kinetic capability and nuclear deterrence
11 programs, we as a country trekked forward without truly
12 understanding the significant changes to the threat
13 landscape.

14 Indeed, only four years later, on February 26th,
15 1993, we witnessed the first bombing of the World Trade
16 Center. I remember it well as I was working in Con Edison's
17 Manhattan Gas Operations Department.

18 Yet again, undeterred, we continued down our path
19 without making fundamental changes to the way our country
20 viewed risk and evaluated threat. As a result, the day of
21 reckoning came eight years later when Al Qaeda murdered
22 2,977 Americans by attacking the World Trade Center on
23 September 11th, 2001.

24 Again, a day I remember well as I was responsible
25 for managing one of Con Edison's control centers. It was

1 only after this avoidable disaster that the Department of
2 Homeland Security was established. Several years later, the
3 Energy's Policy Act of 2005 amended the Federal Power Act to
4 add Section 219, which directed FERC to use transmission
5 incentives to help ensure reliability and reduce the cost of
6 delivered power by reducing transmission congestion.

7 Albeit, this initiative was not focused on
8 national security, but the more than 80 billion dollars of
9 investment added a level of resiliency into the grid, which
10 before enacted, may not have occurred as expeditiously.

11 Ironically, today we have a similar opportunity
12 to leverage the expertise and resources of many of our
13 energy sector partners, however this time, with a goal of
14 maintaining national security.

15 Today, we are keenly aware of high impact,
16 technically-validated threats to our national security.
17 Cyber and physical national state terrorism. These threats
18 are sophisticated, the nation states involved with these
19 threats are insidious, and the consequences of a successful
20 attack could be devastating.

21 According, our previous strategy of maintaining
22 our position in the world through superior kinetic force,
23 may be rendered inadequate by computers operated by
24 malicious nations half a world away.

25 Today we are facing geopolitical challenges from

1 nations whose fundamental principles and ideologies vary
2 vastly from our own. Specifically, the freedoms,
3 transparency and adherence to laws which underpin the fabric
4 of our society have become our Achilles heel.

5 As an example, the Chinese do not recognize nor
6 respect any laws associated with intellectual property, and
7 in fact recently established laws to compel companies to
8 provide otherwise unavailable information to the Communist
9 state whose intent is to leverage this information during
10 times of political tension.

11 To be clear, today we are competing with nations
12 whose goals are nefarious and ruthless. The cyber and
13 physical destruction battlefields for the energy sector is
14 being planned as was highlighted by the Director of National
15 Intelligence during his recent testimony and is included in
16 the 2019 worldwide threat assessment. There is no doubt
17 that nation states have the ability to execute strategies
18 determined to undermine our Democratic institutions.

19 This is the known risk and reality we face. In
20 the face of this adversity we must be proactive, eliminate
21 the threat through strategic risk-informed, cost conscious
22 investments. Simply, we cannot wait until a disaster occurs
23 to develop and execute the strategy to address that known
24 risk.

25 We should all have great intolerance for

1 inaction, especially in the face of reasonably, probable
2 catastrophic events and their likely damaging consequences.
3 I am confident under the leadership of FERC and Chairman
4 Chatterjee, informed by the notable work that has been done
5 by many utilities and the respective regional transmission
6 operators, that we can be proactive and remediate and/or
7 eliminate existing and future threats to our national
8 security and critical infrastructure.

9 In addition, there have been various initiatives
10 by the President's National Infrastructure Advisory Council,
11 the National Academy of Science, the North American
12 Electricity Reliability Corporation, the National Labs and
13 academia that are instrumental in framing the challenge and
14 informing policy-based solutions.

15 We as an industry, have an opportunity to make a
16 bold decision -- deriving from this hearing today. One that
17 will have profound and lasting impact on the energy sector
18 and national security. While others may tentatively watch
19 and contemplate the challenges we presently face, I am
20 inspired by the commitment and vigor the energy industry
21 exemplifies to face an act upon this challenge.

22 Whether it is responding in force as a unit to
23 major natural disasters like hurricanes realized over the
24 last few years or preparing for the inevitable cyber
25 physical battle that is brewing. The energy sector and its

1 leadership are truly inspirational. To my colleagues in
2 the industry, thank you for your unrelenting attention to
3 this very important issue, and thank you for your service to
4 our great nation.

5 CHAIRMAN CHATTERJEE: Thank you, thank you
6 Assistant Secretary. Now, we're going to turn to some
7 remarks from Administrator David Pekoske, Administrator, the
8 floor is yours.

9 MR. PEKOSKE: Okay, thank you Chairman, I
10 appreciate the opportunity to be with everybody today. Good
11 morning to everyone in the audience and on the webcast. And
12 I'd also like to acknowledge the other FERC Commissioners
13 that are here in attendance and Assistant Secretary Walker.

14 A couple things from my perspective and I just
15 want to share a little philosophy at the very beginning.
16 You know, I firmly believe that good security is at the end
17 of the day a partnership and when I look at security from a
18 transportation security administration perspective, I know
19 that I can't provide the security that our nation requires,
20 were it not for the close work and the close working
21 relationships we have with our partners.

22 And I would include in our partners, the Federal
23 Energy Regulatory Commission, the Department of Energy and
24 one aspect of the Department of Homeland Security, which is
25 relatively new on the horizon and that's the Cybersecurity

1 and Infrastructure Security Agency or CISA, that is a key
2 partner of TSA's in providing cyber security in particular,
3 across a spectrum of our responsibilities.

4 I would also note that from my perspective,
5 safety and security are really two sides of the same coin.
6 And we work very, very closely with the Department of
7 Transportation. As many of you know, the Transportation
8 Security Administration, transportation -- the first word in
9 our name, was born in the Department of Transportation and
10 we've maintained those relationships and they are very
11 strong.

12 But across the board, whether it's in the
13 aviation sector or the surface transportation sector, we
14 have, I think, a very open and collaborative and very
15 cooperative relationship with all of our partners. All of
16 our partners in industry as Bruce was describing, and our
17 partners at the state and local government level.

18 And really, with respect to surface
19 transportation security, the topic of this morning's event,
20 and specifically with pipelines, we need to have very strong
21 relationships with the industry. I think we do, and
22 certainly with the state and local governments around the
23 country.

24 As many of you know, TSA was formed right after
25 911. In fact, the law that establishes TSA is the Aviation

1 and Transportation Security Act and it was signed by
2 President Bush on the 19th of November in 2001. While most
3 people identify TSA with aviation security, and that is the
4 lion's share of the men and women who formed TSA.

5 We also have significant responsibilities for
6 surface transportation security. And, you know, the
7 difference between aviation security and surface
8 transportation security for our agency is that we provide --
9 we actually provide the security in the aviation sector in
10 the surface transportation security sector. We work very
11 closely with state and local governments and owners and
12 operators in systems around the country.

13 I would tell you that from my perspective, I've
14 been in this position for a little over a year and a half.
15 I have placed significant emphasis on the pipeline industry
16 -- 2.7 million miles of pipelines around our country, 3,000
17 companies involved in it overall.

18 And I think we have put forth significant effort
19 from the Transportation Security Administration to ensure
20 that we are up to speed with pipeline security issues, and
21 I'm going to describe some changes in a second that we have
22 already underway within TSA.

23 Before I do that, I would just invite anyone to
24 visit our website, and on our website, you will see several
25 documents that will give you a sense of where we're going as

1 an agency. We have a TSA strategy that was published about
2 a year ago. Accompanying that strategy is a document called
3 the administrators intent, which is my personal document
4 that says hey, given the strategy for TSA, this is my intent
5 as the current administrator on how I'm going to advance the
6 specific strategic objectives for the agency while I'm in
7 this position.

8 Additionally, there are pipeline security
9 guidelines posted on our website, as well as our cyber
10 security roadmap. I felt it was very important that we put
11 documents in place early on in my tenure, but every single
12 one of those documents was put together not by TSA and not
13 by TSA alone, but in very close collaboration with all of
14 our stakeholders, whether they were other government
15 agencies, whether they were industry partners or members of
16 Congress and their staffs, or international partners.

17 And so, I would just invite folks, you know, if
18 you have the time look at the TSA website, and that will
19 give you a sense of where the agency is going overall.

20 To execute on the above though, you know, when I
21 came into this position I said hey, I'm not going to come in
22 and do a bunch of restructuring in the agency without really
23 understanding the agency, and without really understanding
24 where we all felt the agency needed to go into the future,
25 but we are at that point.

1 And we are making some structural changes within
2 TSA. In a simple way of looking at it, we are doing a
3 couple of things that really definitely impact the pipeline
4 security mission that we have. The first is we are putting
5 all of our policy-making into one policy stop.

6 We are not going to have multiple policy shops in
7 the agency. I think that there's a lot to be learned from
8 security in other sectors that apply across the board, so
9 all of our policy is going into one place. And importantly,
10 all of our operations are going into one place.

11 With that we'll result in, with respect to
12 pipeline security, is a greatly expanded reach of our
13 pipeline security staff, and a much larger staff overall to
14 be able to accomplish that mission. The staff in surface
15 transportation security will now have direct control of our
16 inspectors stationed throughout the country in airports
17 throughout the country because what we have is 440
18 federalized airports -- TSA is present in every single one
19 of those airports.

20 We put all of our inspectors on the airport
21 staffs, but we're going to make a change to that and we're
22 going to take the inspectors that are designated for surface
23 transportation security and put them directly under the
24 Surface Transportation Security Assistant Administration, so
25 there's direct reach and direct regional and local reach

1 across the entire organization.

2 Additionally, we are also going to work very hard
3 on establishing a regional presence and as we establish a
4 regional presence, we already have it in place right now,
5 it's primarily purposed to support our aviation security
6 mission. I'm re-purposing that to do two things -- to
7 advance the surface transportation security mission, and to
8 also advance our contingency and planning response
9 capability.

10 And so, our regional presence will be co-located
11 with five FEMA regions around the country and located in
12 cities like New York, Atlanta, Chicago, Dallas and Seattle.
13 The other thing that we are working on very hard is to
14 invest in more cyber specific expertise within the agency.
15 We rely a great deal on the Cybersecurity Infrastructure
16 Security Agency, CISA, that I mentioned at the beginning of
17 my remarks, but it's my desire to have specific
18 industry-related cyber security expertise within TSA.

19 And, you know, this will be leveraged off of our
20 existing cyber security expertise within our information
21 technology division within the agency which is quite
22 substantial. Let me conclude by just emphasizing what I
23 started out with.

24 Is, you know, I think strong partnerships are the
25 keys to all of our success in the future and I think by

1 strong partnerships we will be able to achieve integrated
2 and continuous improvement. This is a fast-moving area of
3 business, a fast-moving area of security, and we need to
4 keep pace with it.

5 In fact, if you look at the TSA strategy, one of
6 the -- there's three strategic priorities, the second of the
7 three strategic priorities is to accelerate action in the
8 part of what we do because I want to make sure that we don't
9 respond at the pace of government, that we respond at the
10 pace of what the mission requires.

11 We will continue to work very closely with our
12 industry partners on security plans, on sharing best
13 practices on exercises and training, and all of these are
14 going to be topics of the panel that will follow opening
15 remarks.

16 I'm a firm believer in information exchange. And
17 finally, what I would want to impart on everyone is that I
18 believe very strongly, that relationships are critical to
19 success and that's why I think this particular event is so
20 valuable. You know, I think it's very valuable that we have
21 a face-to-face dialogue. We understand each other's
22 positions and then together we can improve security overall
23 which is I think the mission of everybody here at this
24 conference and everybody here on the webinar.

25 So, with that, thank you very much for the

1 opportunity to speak. Thank you for the opportunity to be
2 here this morning and I look forward to the panel. Thank
3 you.

4 CHAIRMAN CHATTERJEE: Thank you Administrator and
5 thank you again for being here. Now, we'll turn to my
6 colleagues for their comments.

7 COMMISSIONER LAFLEUR: Thank you Mr. Chairman, I
8 also want to welcome everyone to this Technical Conference,
9 especially our guests from sister federal agencies and from
10 the state agencies who we will be hearing from as well as
11 everyone participating in the panels and in the audience.

12 One of the things that struck me time and time
13 again in the last 9 years is how complicated government is.
14 I probably should have learned that in the 5th grade, but I
15 don't think I really figured it out until I was part of the
16 government.

17 And as today's guest list illustrates, the
18 nation's energy infrastructure is regulated, and its security
19 protected by a complex and at times overlapping set of
20 agencies at the federal and state level. And in order for
21 us to best work together to assure that critical
22 infrastructure is secure for the benefit of customers who
23 rely on it, it's very helpful to have shared priorities
24 among all the federal and state policymakers who use pieces
25 of our jurisdiction to influence grid security and other

1 energy security.

2 So, I thank the Chairman for pulling together
3 this Conference with Secretary Walker, and I'd like to thank
4 our
5 Director of the Office of Energy Infrastructure Security,
6 Joe McClelland and his team, Carolyn and Annie, and the
7 others for all their work on pulling this complex thing
8 together.

9 In the case of FERC, our primary relevant
10 jurisdiction is to oversee the establishment and enforcement
11 of the set of mandatory reliability standards for the bulk
12 electric systems, both transmission and generation to
13 prevent cascading outages or uncontrolled separation of the
14 grid.

15 We also of course, have great authority over
16 transmission, on wholesale sales of electricity and gas and
17 oil pipelines. Congress gave us the standards authority in
18 2005 in the same law that's been referred to, specifically
19 including the responsibility to oversee standards to prevent
20 cyber security incidents.

21 At that time Congress also required us to allow
22 full cost recovery for actions that registered companies had
23 to take to respond to the standards. Since that time, FERC,
24 NERC, represented by Jim Robb, the regional entities and the
25 electric industry have worked hard to put in place a

1 comprehensive set of mandatory standards.

2 In the past several years we've particularly done
3 a lot of work on grid security -- several generations of
4 cyber security standards, including most recently a heavily
5 debated supply chain standard as well as standards related
6 to physical security and geomagnetic disturbances.

7 Those standards are the backdrop for the way we
8 look at today's Conference, but in fact the Conference is
9 about how we can and should go beyond them and work
10 collectively to address the security of other interdependent
11 infrastructure networks, such as natural gas.

12 In addition to what's been mentioned, there's
13 really three things I'd like to focus on. The first is with
14 respect to the bulk electric system -- so, we have these
15 standards, but what efforts beyond the standards do we need
16 to collectively work on?

17 For example, this week there was an executive
18 order issued on electromagnetic pulse. What are the things
19 we should be doing that aren't in the standards and maybe or
20 maybe not -- should not be in the standards, but how do we
21 work on the other things?

22 The second thing -- and do things more quickly
23 than the standards process allows. Secondly, since FERC
24 oversees transmission security and transmission rates, and
25 the states oversee distribution security and distribution

1 rates, and one of the things I learned when I ran a
2 distribution company is they're like actually attached in a
3 million places, how can we work together in a complimentary
4 fashion to ensure that the whole grid is secure for
5 customers?

6 We talk about it a lot, but it's very hard to
7 figure it out. And thirdly, how can we work together to
8 ensure the security of all the interdependent infrastructure
9 -- electric, gas, oil, water, telephone, that needs to work
10 together because it's, you know, the weakest link and all
11 that.

12 That's a big task, but those are some of the
13 things I hope we can get into in the conversation, and I
14 hope we'll end the day with some concrete suggestions for
15 action, thank you.

16 COMMISSIONER GLICK: Thank you Mr. Chairman, and
17 I want to join my colleagues first in welcoming our
18 government partners here, Secretary Walker, Deputy Assistant
19 Secretary Hoffman, and Administrator Pecoske, I really
20 appreciate you being here today and I think we're going to
21 learn a lot. And I also want to commend you Mr. Chairman,
22 because I know since you've been here at the Commission,
23 that you have made cyber security one of your top
24 priorities and a top priority for the Commission and it's
25 very important obviously that we do so for the reasons that

1 have already been mentioned, but I think, you know, everyone
2 knows that you really can't open up a newspaper or turn on
3 the cable news show these days without seeing a story about
4 cyber attacks against our critical infrastructure, including
5 obviously our electric grid and natural gas pipelines and
6 some concern.

7 We have great concern about that and then
8 Assistant Secretary Walker mentioned, I think, very
9 correctly the Director of National Intelligence Coats'
10 remarks before the Senate Intelligence Committee in January,
11 and you know, basically you can't listen to those remarks
12 and not understand that the Russians, the Chinese and
13 several other nations are using the internet in a variety of
14 ways to attempt to undermine our economy and our politics,
15 our very way of life, and so this is obviously an extremely
16 important issue.

17 We have a lot of panelists here today and a lot
18 of people still to make speeches, but I don't want to take a
19 lot of time, but there are two issues that I'd really like
20 to hear more about today. And one of them is, as
21 Administrator Pecoske talked about, how we address our cyber
22 security of our national gas pipeline system.

23 Chairman Chatterjee and I last year did an op-ed
24 in the Houston Chronical expressing concerns about
25 government overview or government regulation of natural gas

1 pipeline cyber security, because not only it's important
2 from a perspective of gas pipeline customers, but also for
3 the electric grid and our responsibilities with regard to
4 the bulk power system.

5 And then, you know, last year in December there
6 was a JO report and it was entitled, "Actions Needed to
7 Address Significant Weaknesses in TSA's Pipeline Security
8 Program Management." And Administrator Pekoske mentioned
9 some tips of the significant changes that are going to be
10 made and I think we need to understand those better.

11 And I want to emphasize first of all, I think we
12 all owe a great deal of gratitude to Administrator Pekoske
13 and also obviously the many thousands of people that work
14 around the country that protect us at airports and bus
15 stations and railroad stations and so on, they do an
16 extremely important job.

17 And I just think we need to do a better job -- we
18 need to get a better handle on whether the TSA -- TSA's
19 responsibilities with regard to natural gas and oil
20 pipelines as well and other hazardous material pipelines,
21 whether we're actually -- we have a good handle on that
22 whether we're actually addressing the cyber security
23 challenges that that faces today.

24 Because as I mentioned, it not only affects gas
25 customers, it affects electric customers as well. The

1 second area I'd like to hear more about today is the issue
2 of incentives and incentives versus standards -- setting
3 standards for instance. So, for instance we're going to
4 talk a lot about whether there are -- whether sufficient
5 investments are being made, or if they're not, what the
6 barriers are to those investments and whether the Commission
7 needs to -- Commission and state regulators will need to
8 provide incentives for the utilities to make those proper
9 investments.

10 I think it's important and we need to take a look
11 at that, but I'd also want to take a look at whether if we
12 think those investments really need to be made, whether we
13 should actually pursue additional standards through the NERC
14 process, and admittedly it is sometimes time consuming, but
15 I think we need to take a look at that as to whether -- and
16 that might be the better approach versus actually just
17 setting a bunch of incentives, not knowing whether the
18 companies are going to make the investments that they need
19 to make to protect our grid.

20 So, with that I'll leave it for everybody else,
21 but I do think we're going to have a very interesting day,
22 and I thank you again for organizing this proceeding.

23 CHAIRMAN CHATTERJEE: Thank you, Commissioner
24 McNamee?

25 COMMISSIONER MCNAMEE: Thank you Mr. Chairman,

1 and thank you to everybody for coming here and it's
2 especially good to see some of my old friends from the
3 Department of Energy. Thank you also for joining us and the
4 panelists as well. You know the issue of cyber security and
5 physical security in our energy infrastructure is vitally
6 important, we all hear it, but this growing awareness of
7 this threat that's coming against us, not just a threat, the
8 actual attack is out there and it's from you know, hostile
9 foreign governments, adversarial competitors and also from
10 rogue terrorists.

11 You know, everybody's mentioned you know, Dan
12 Coats, the Director of National Intelligence, you know,
13 making a statement in January of 2019. I also recall he
14 gave a speech back in July of 2018 in which kind of
15 referring to 911 he said the lights are blinking red again.

16 And I think that is something that we really need
17 to be worried about. And just a short review will remind us
18 of why this Conference is so important. A year ago, in
19 March 2018, the Department of Homeland Security and the FBI
20 issued an alert and stated, "That since at least March 2016,
21 the Russian government cyber actors targeted government
22 entities in multiple U.S. critical infrastructure sectors,
23 including the energy, nuclear, commercial facilities, water,
24 aviation and critical manufacturing centers.

25 We also learned that certain pipeline data

1 systems had been hacked by unknown actors about a year ago.
2 We've seen the constant news stories about how China, Iran,
3 North Korea, Russia -- all them have been targeting our
4 entire economy, in particular, energy infrastructure.

5 We also realize that it's not just cyberattacks,
6 that are a problem which is why this is about energy
7 infrastructure security, including physical. There was the
8 attack on the Metcalf substation. We've seen that there's
9 been attacks on other transformer immersion substations.

10 Another thing that we realized, and we've been
11 trying to deal with is the supply chain issue, when
12 virtually every device now has a little chip in it, if
13 you're getting your chip from overseas, is there something
14 in there that makes us vulnerable?

15 And then, as Commissioner LaFleur referred to,
16 the President just this week talked about EMP. The purpose
17 for listing all these things is saying that the threats are
18 many, and they come in many different places, and that we
19 have to have a wide threat analysis and understand that it's
20 not just one thing, it's not just tweaking one standard, it
21 is a problem that permeates virtually every aspect of what
22 we do in our economy.

23 And of course, government has a significant role
24 to play in this, but it's not just the role of FERC or of
25 DOE, or TSA or the Department of Defense, or even the

1 private sector. It is all of us having to be vigilant and
2 having to deal with the issue. It means individuals,
3 whether it's employees who are at FERC, whether it's me as a
4 Commission or not, clicking on something, whether it's
5 employees, you know, at a substation making sure that
6 they're in compliance with the requirements of their
7 utility.

8 All of us have an obligation to be vigilant
9 because it's all of our collective security. I think that's
10 why it's important that we gather here today because we've
11 seen what can happen if there's a massive loss of power.
12 Think about what's happened in Puerto Rico with Hurricane
13 Maria -- we know that Assistant Secretary Walker spent much
14 time out there trying to help them deal with the power
15 outages there.

16 Think in 2003 with the Northeast Blackout and
17 what it did to so many people who were left without power.
18 And these are things that you know, you can look at, oh you
19 know, natural disasters that's hard, but shame on us if we
20 are not vigilant to try and stop the intentional acts
21 against us and to be vigilant about it.

22 So, as we go through today, we're going to be
23 talking about a variety of things -- not just the threats,
24 but also the incentives. How do we deal with the
25 fundamental and practical challenges of cost recovery?

1 Those are important issues, and those are things that we
2 need to figure out and they are things that are going to
3 have the intersection between -- as Commissioner LaFleur
4 stated, between federal cost recoveries, state cost
5 recovery.

6 It's going to take a requirement of all of us
7 rethinking how we approach challenges and problems in order
8 to make sure that we guarantee and are able to protect the
9 quality of life that's not just about you know, dollars and
10 cents. It's about keeping the hospital running, it's about
11 the daycare center being in operation, it's about being able
12 to have our elderly parents continuing to be safe in a
13 senior facility.

14 These are real issues that deal with real life
15 and we've got to be vigilant about it and work forward and
16 so I applaud the Chairman for gathering us together and for
17 everybody here for their willingness to work through this,
18 and I know that together we'll be able to tackle this issue,
19 thank you.

20 CHAIRMAN CHATTERJEE: Thank you Commissioner
21 McNamee. This dialogue today would not be possible without
22 the tremendous work of our Office of Energy Infrastructure
23 Security. Thank you, Joe McClelland, to you and your team
24 for your leadership on this and I will turn it over to you
25 for some housekeeping.

1 PANEL 1: Cyber and Physical Security, Best Practices, and
2 Industry and Government Engagement.

3 MR. MCCLELLAND: Thank you, let's begin by asking
4 the remaining panelists to please join the table. And thank
5 you Mr. Chairman and to our guests. Welcome to the Federal
6 Energy Regulatory Commission. Let's begin with a few
7 housekeeping items.

8 First, food and beverages with the exception of
9 water are not permitted in the Commission meeting room or in
10 today's case, the overflow hearing rooms.

11 Second, please silence all cell phones, and now
12 would be a good time to do so.

13 Third, to our panelists. Please remember to turn
14 on your microphones before speaking and very importantly, to
15 turn them off when you're done speaking.

16 And finally, we will be breaking for lunch at
17 12:30 today. Members of the public are invited to observe,
18 which includes attending, listening and taking notes, but
19 does not include participating in the Conference or
20 addressing the Commission.

21 Actions that purposely interfere or attempt to
22 interfere with the commencement or conducting of the
23 Conference or inhibit the audience's ability to observe or
24 listen to the Conference, including attempts by audience
25 members to address the Commission while the Conference is in

1 progress are not permitted.

2 Any person engaging in such behavior will be
3 asked to leave the building. Anyone who refuses to leave
4 voluntarily will be escorted from the building. Finally,
5 while there is no general question and answer session with
6 the audience during today's conference, the Commission will
7 be accepting written post-technical comments in this
8 proceeding.

9 Expect to see a formal invitation for those
10 comments which will include submission deadlines in the near
11 future. The purpose of this Technical Conference is to
12 discuss matters set forth in the noticed agenda. We do not
13 intend for this Conference to address proceedings that are
14 currently pending before the Commission, including
15 proceedings that touch on cost recovery or other matters
16 that may relate to today's discussion.

17 Consistent with the purpose of this Conference,
18 and to ensure compliance for the Commission's ex parte
19 rules, we ask that all speakers today refrain from
20 discussion of any contested proceeding that is currently
21 pending before the Commission. David Morenoff, from the
22 Office of General Counsel is here to help ensure that no ex
23 parte communications take place, there's David.

24 In addition to ex parte matters, please do not
25 discuss any information that could be considered sensitive

1 or classified. Finally, we have a slight adjustment to
2 today's panel. We were informed this morning that Bob
3 Kolasky, the DHS National Risk Management Center cannot join
4 us as he has fallen ill. We will miss him and wish him a
5 speedy recovery.

6 Now the directions to our panelists -- as you
7 know we have a very robust agenda and keeping on schedule's
8 important. Therefore, please introduce yourselves,
9 including your title and your organization. Please notice
10 that there is a time clock on the floor which will begin
11 counting when you start your remarks, and please limit your
12 statements to five minutes, remembering that there may be
13 additional time to discuss your topics during the question
14 and answer session.

15 Now, to our first panel. This panel will discuss
16 types of cyber and physical security throughout the energy
17 infrastructure, particularly electric transmission
18 generation and natural gas pipelines.

19 In addition, the panel will explore best
20 practices for cyber and physical mitigation beyond those
21 measures already required by managed or reliability
22 standards -- what industry and government engagement is
23 needed to address these matters.

24 At this time, I'd like to turn over the
25 microphone to our first panelist, my good friend Mr. Bill

1 Evanina, Bill the floor is yours.

2 MR. EVANINA: Thank you Joe, Commissioners,
3 Chairman, distinguished experts, it's a great pleasure for
4 me to be here. I'm the Director of the National
5 Counterintelligence and Security Center. My boss is
6 Director Dan Coats and I'm humbled to be here to represent
7 the men and women of the intelligence community, the entire
8 government who work diligently every day to protect our
9 national security, specifically with respect to
10 counterintelligence and security threats.

11 As part of this panel, I think it's really
12 important to focus on some of the comments already made by
13 the Commissioners with respect to the criticality of
14 integration coordination, communication and partnership. I
15 think the term "public private partnership," gets used way
16 too often without exact meaning.

17 And I think in this particular venue it's more
18 important with respect to energy than ever before and I'm
19 going to lay out some reasons why. As the Director of the
20 National Counterintelligence Security Center, we have an
21 obligation to put forth the national strategy for
22 counterintelligence to the President, and we're in final
23 coordination to do that.

24 I want to provide a juxtaposition as to where we
25 are with that right now and why it matters to this room.

1 So, in 2016 we issued the counterintelligence strategies for
2 the President and those pillars of priorities were China,
3 Russia, Iran, North Korea and a subset of others. It sounds
4 logical, it sounds normal.

5 Just three years later it's important to know how
6 vast and how substantial the change of construct is with
7 respect to the counterintelligence threat. The pillars that
8 will be going to the President right now are the following:

9 Number 1 -- critical infrastructure.

10 Number 2 -- supply chain, and

11 Number 3 -- cyber.

12 If you think about the transition in just three
13 years, and the prospects of where we are, the biggest change
14 in I will call it transformational mindset and management
15 paradigm shift, will be the requirement to protect our
16 nation is now transforming beyond the federal government and
17 intelligence community to the private sector to academia, to
18 the business community, to small and local businesses and to
19 be able to protect our power grids, our pipelines we talked
20 about as well as our telecommunications and financial
21 systems.

22 This is now a whole country approach to defending
23 our nation from nations and threat actors. And some of the
24 Commissioners mentioned already that comments by my boss Dan
25 Coats. I think it's really important and I want to read a

1 few of the comments aloud if I might, because what goes into
2 this annual threat assessment is not a small thing.

3 It is a compilation of really sensitive documents
4 that are acquired through multiple means around the world
5 that I put together in a document in an unclassified manner.
6 But I think if you listen to the words carefully, you could
7 really get a sense of the vileness, the pervasiveness and
8 the enduring threat we face through our nation's threat
9 actors which I really want to specify are China, Russia,
10 Iran and North Korea.

11 Just to read a few, China has the ability to
12 launch cyber attacks that cause localized, temporary
13 disruptive efforts on critical infrastructure such as
14 destruction of natural gas pipeline for days to weeks.
15 There's a reason why that was in the report.

16 Russia has the ability to execute cyber attacks
17 in the United States that generate localized, temporary
18 disruptive effects on critical infrastructure such as
19 disrupting an electrical distribution network for at least a
20 few hours.

21 Similar to those demonstrating nuclear in 2015
22 and 2016, there's a reason why that sentence was in there.
23 Iran has been preparing for cyberattacks against the United
24 States and our allies. It is capable of causing localized
25 temporary disruptive effects such as disrupting a large

1 company's corporate network for days to weeks.

2 We cannot minimize the words that are in that
3 statement. They're in there because there's lots of
4 intelligence behind every sentence in that report.
5 Intelligence that we know our adversaries are planning,
6 they've already done, their efforts successfully, with
7 respect to ISC and SCADA systems, they're trolling their
8 surveillance of our grid system, our gas pipelines, our oil
9 pipelines, the transportation system that Mr. Pekoske talked
10 about is a priority for adversaries.

11 We in the government have to be more effective
12 and efficient across multiple means to be able to drive the
13 threat and vulnerability as we see it from collection to the
14 owners of those utilities and pipelines and to the
15 regulators and to the government agencies who oversee and
16 protect the criticality of our energy.

17 The top three critical infrastructure areas we'll
18 look at are energy, telecommunications, and financial
19 systems. I will prophet to you none of the other two worked
20 without energy. There was a reason why when we look at our
21 threat posture across the country and our energy facilities,
22 our military bases, our weapons systems, our critical loads
23 of communication and we see our adversarial intelligence
24 officers and non-traditional collectors going to those
25 locations but not into the military base -- to where those

1 military bases are powered.

2 Where is the power that's being generated to
3 supply that military base? That energy facility? We have
4 to be able to be joined at the hip with respect to what that
5 threat is, how the vulnerabilities manifested and more
6 importantly who owns the consequence? We all do. And if we
7 think about why it matters, we must only think about what
8 if.

9 And I think with the partnership we have with
10 FERC, DOE, DHS, FBI, NSA, we will continue to drive that
11 threat and awareness through the CEOs of the energy world so
12 we could better as a team, prepare our nation for safety.
13 Thank you for your time.

14 MR. MCCLELLAND: Thank you Bill, Chuck, the
15 microphone's yours.

16 MR. KOSAK: Great, thank you. My name is Charles
17 Kosak. I'm the Deputy Assistant Secretary of Defense for
18 Defense Continuity and Mission Assurance. I wanted to start
19 by just saying it's an honor to be here. I also wanted to
20 just express my condolences to the FERC family for the loss
21 of Kevin McIntyre.

22 My wife was a running buddy of his and we had the
23 regretful, but honor to attend his funeral recently, so my
24 condolences. I'm going to start by talking a little bit
25 about the strategic aspect of this.

1 The DNI briefing was kind of my quadruple
2 espresso as I move into my comments. And I'll talk a little
3 bit about the NDS, and then I'd like to talk about our
4 defense critical electric infrastructure efforts with DHS
5 and DOE and why we deem that to be such a critical endeavor.

6 So, it's not going to come as a surprise to
7 anyone, especially recently having Assistant Secretary
8 Shanahan and the Chairman of the Joint Chiefs of Staff brief
9 the Senate Armed Services Committee on the DOD budget.

10 But if you notice in those remarks, a very
11 prominent feature had to do with the symmetric as well as
12 the asymmetric elements of what DOD does for a living. When
13 we talk about symmetric military capabilities, we're talking
14 about those capabilities that exist above the threshold of
15 war.

16 We're talking about those capabilities in which
17 both China and Russia and others constantly engage in a
18 military buildup and constantly seek to modernize their
19 capability and capacity for war.

20 Equally as much, we have deterrent elements that
21 are affective in that realm. The critical piece of all this
22 is the asymmetric or hybrid warfare piece and when you look
23 at Russia, Russia's developing exquisite capabilities not to
24 scale, and China's building increasingly very modernized
25 capabilities increasingly to scale.

1 And, but both nations realize that the United
2 States maintains a qualitative military edge in this arena
3 and very excellent deterrence capacities. What both are
4 interested in among other countries that have been mentioned
5 today -- Iran, North Korea, is to introduce the means by
6 which they might be able to impact our communications or
7 impact our energy -- the flow of energy or impact other
8 areas where really the musculature of how the Department of
9 Defense moves assets and people and builds lethality in the
10 world to do the nation's business.

11 The reality is that they're making lots of
12 progress and when you look at the national defense strategy,
13 it's comprised of four layers. The first layer is contact.
14 The second layer is blunt. The third is surge and the
15 fourth is homeland defense. And we delineated these layers
16 in the national defense strategy so that we could better
17 risk manage our assets, networks, systems and platforms and
18 better prioritize how we execute our operational plans and
19 contingency plans.

20 And the thing I want to stress today,
21 particularly after the DNI briefing is that we have the
22 adversaries who are, in fact, targeting our critical
23 infrastructure and they're targeting civilian as well as
24 military critical infrastructure.

25 Many of you know that most of the defense

1 critical infrastructure of which we depend is not owned or
2 operated by the Department of Defense, you know, hence the
3 criticality of strengthening -- I would even say
4 operationalizing these partnerships.

5 We're at a point in time where theorizing about
6 the threat at a time where observing and reacting to the
7 threat is getting late to need. We need to be anticipatory.
8 We need to anticipate where our adversaries are going and
9 take action to collaborate and partner in these areas right
10 now. So, this is a critical piece of us. The other -- the
11 last piece I have 47 seconds, I want to make is -- we're
12 better at this than ever before.

13 I mean I'm surrounded by a lot of people who know
14 a lot more about electricity than I do. I know we just need
15 it. And people who are business people, you have customers,
16 you have responsibilities, you make investments on a daily
17 basis. You face shareholders that hold you to an exacting
18 accountability and so the point in all this is DOD isn't
19 just leveeing requirements now.

20 We have a risk management construct that is very
21 dynamic. The Chairman has announced defense critical
22 missions and so we pull a thread with every single
23 operational plan, whether it's nuclear community control
24 communications or ballistic missile defense, we are
25 dynamically working together to rack and stack single points

1 of vulnerability, identify them very clearly, try to plan
2 around them as the most cost-effective way, find alternative
3 ways and means to get to that same op plan end, and where we
4 can't, we need to remediate through investments and build
5 redundancy and partner with DHS, partner with DOE, and
6 partner with industry in the private sector.

7 So, you can feel assured as we partner with you
8 that we're not just dumping requirements. We put a lot of
9 strategic operational and tactical fun into these things, so
10 you're getting a return on investment insofar as investing
11 in our ability to defend the U.S. and protect the American
12 people, thank you.

13 MR. MCCLELLAND: Thank you Chuck, Sonya?

14 MS. PROCTOR: Good morning and thank you Chairman
15 Chatterjee and Commissioners and our other distinguished
16 panelists. Thank you for the opportunity this morning.

17 TSA has had great success in working with the
18 pipeline community to develop and implement voluntary
19 guidance and programs to enhance overall security in the
20 pipeline industry. Specifically, the pipeline community has
21 been very engaged in the development of our pipeline
22 security guidelines, including the addition of a new
23 comprehensive cyber security section with the most recent
24 addition of the guidelines.

25 These guidelines serve as the de facto standard

1 for pipeline security programs and were developed in close
2 coordination with our pipeline security partners and our
3 government partners as well.

4 Major pipeline industry associations continue to
5 show support and -- support for, and collaboration with the
6 measures set forth in the guidelines. Associations, such as
7 the American Gas Association, the Interstate Natural Gas
8 Association of America, and the American Petroleum Institute
9 have written what they call membership statements committing
10 to voluntary adherence to the pipeline security guidelines.

11 Pipeline operators have shown a willingness and
12 ability to voluntarily implement the mitigation measures set
13 forth in the guidelines. We have strong indicators that
14 an industry-backed voluntary program to reduce risk by
15 increasing compliance with the guidelines is working.

16 Among our efforts, TSA conducted 23 corporate
17 security reviews in fiscal year 2018, and those pipeline
18 operators assessed hitting 90% adherence rate regarding
19 corporate security program management. An 85% adherence
20 rate regarding security incident management, and an 80%
21 adherence rate regarding TSA recommended cyber security
22 practices detailed in the 2011 guidelines.

23 In addition, we've seen a strong increase in the
24 level of corporate adherence to the guidelines when
25 comparing results from a second review to the company's

1 first review. For ten companies where we conducted a second
2 corporate security review, we've seen the number of
3 recommendations made decrease from a total of 446
4 recommendations that were made collectively from the first
5 review to 146 during the second review.

6 In addition, companies have implemented
7 corrective actions on over 81% of the recommendations made
8 during our critical facility security reviews. This is
9 indicative of industry's acceptance of and adherence to, the
10 TSA pipeline security guidelines.

11 Now, with the support of the Cybersecurity and
12 Infrastructure Security Agency, CISA, and the National Risk
13 Management Center, and their cybersecurity expertise, we've
14 undertaken a new level of cybersecurity reviews in the
15 pipeline industry to better identify and mitigate risks
16 associated with pipeline operations.

17 So, Mr. Chairman, I want to thank you for your
18 continued support of the Joint Cyber Architecture Reviews
19 that we've conducted along with Director McClelland and his
20 team -- those were the very first cyber architecture reviews
21 that we conducted, and that gave us a great start. We're
22 now continuing those reviews under the National Risk
23 Management Center, and we're looking forward to a continued
24 partnership here.

25 So, thank you so much for your support and the

1 support of our partners around the table here, and we look
2 forward to continuing to share information today, thank you.

3 MR. MCCLELLAND: Thank you Sonya, Nick?

4 MR. AKINS: Thanks Joe, first of all thank you
5 Chairman Chatterjee and Commissioners, to our government
6 partners as well and colleagues. This is an important time
7 in our industry and I really believe that we are the new age
8 of resiliency and reliability being a critical component of
9 every decision that we make.

10 And whether it's man-made or whether it's -- well
11 weather related or any of those factors, these are
12 cross-cutting issues no matter what we do and really is a no
13 regrets type of strategy for our company and this industry
14 to focus on these types of efforts.

15 And certainly the CIP standards provide a firm
16 foundation, we're the only industry that has those
17 requirements and certainly for us we want to continue that
18 and continue the growth of that because it's incredibly
19 important for us to be able to move forward with regulatory
20 recovery and all those aspects that we're doing in the
21 background to ensure that we are doing the right thing.

22 My name is Nicholas Akins, Nicholas K. Akins, I'm
23 Chairman, President and CEO of American Electric Power, one
24 of the largest electric utilities in the country and we
25 certainly feel like we have a role to play in terms of our

1 ability to serve our customers, particularly customers that
2 are demanding more electrification of the economy that's
3 occurring and we need to make sure that we have that
4 backbone in place to serve our customers in the future.

5 I also will tell you that our Board is incredibly
6 focused on these issues and I don't think you'll find an
7 industry board that isn't in this point in time on
8 cyber-related, physical-related activities, but also risk
9 and risk management associated with any of these types of
10 issues and impact the resiliency and reliability of the
11 grid.

12 So, I really believe that as we move forward
13 there's four areas, I think that are particularly important.
14 One is we are an ever-changing landscape, and we're
15 certainly seeing on a regular basis -- so regular in fact
16 that I have regular meetings with our cyber and physical
17 security efforts to get routine updates on whenever, and
18 well sometimes that date happens anyway, but on a regular
19 basis though, really focused on where they're coming from,
20 but also focus on the ability for us to work with our
21 government partners because a lot of information we get are
22 from these partners and certainly that's a clear issue for
23 us and the industry to really focus on the advancement of
24 these partnerships and there are several avenues for doing
25 that -- Electric Sub Sector Coordinating

1 Council certainly is one.

2 But also, there are others and we need to focus
3 on those, but also the focus on our regulators as well. And
4 we, obviously have, we're in 11 states, and state regulators
5 are also important because they review the costs of these
6 types of activities but there's no question that we do have
7 the support of our state regulators as we go through these
8 types of processes.

9 And then also the interdependencies related to
10 the grid itself, and certainly natural gas as we depend more
11 upon natural gas, we'll certainly be one of those areas that
12 we need to take a close look at, but I also raise up to you
13 the ability for transmission to get built in this country,
14 to provide that backbone interface that occurs across the
15 country and bring resources in where they're needed to be,
16 but also there's a reason for a balanced energy portfolio.

17 And as we focus on those types of issues, it's
18 incredibly important to think about that in the context of
19 resilience and reliability of the grid and Commissioner
20 McNamee, you brought up the 2003 blackout. A lot of the
21 prime moves in place, the large generation stations and the
22 transmission in the areas stopped the cascading of those
23 events. So, we need to learn from those but certainly the
24 resiliency and reliability of the grid relative to cyber and
25 physical security are important.

1 The other is infrastructure hardening. There's a
2 lot of efforts being placed in the industry relative to
3 continued development of not only hardening of facilities,
4 spec'ing out the design of additional facilities, but also
5 ensuring that we're addressing the multitude of threats that
6 exist, whether weather-related, whether EP related, and
7 certainly I think when you think about incentives in the
8 industry, and I know FERC is reviewing incentives, it's
9 important for transmission and other types of factors
10 relative to cyber and physical security to be done from an
11 incentive perspective.

12 I mean that's the subject of the next one. So,
13 I'll just stop now, okay, I'll stop with that. Have I done
14 my five minutes already? 17 -- second? Okay, so as we look
15 forward to many of the things that we're doing in our
16 industry, I think it's really important for us to have that
17 communication with our government partners, our regulators,
18 but focus in on examples because those examples really do
19 show us the path toward the future as well, in terms of that
20 development.

21 MR. MCCLELLAND: Thank you Nick, sorry about the
22 30-second warning there.

23 MR. AKINS: I get that all the time.

24 MR. MCCLELLAND: Mark, the floor is yours.

25 MR. GABRIEL: Great, thank you. I'm Mark

1 Gabriel, I'm the Administrator and Chief Executive Officer
2 of the Western Area Power Administration and I'd like to
3 give you a little bit of context first, thank you very much
4 for including us.

5 WAPA's footprint is 1.4 million square miles
6 across 15 states, so the equivalent of going from Paris to
7 Moscow and Athens to Oslo, if you think about it, with all
8 the same politics in between by the way.

9 And we're very unique in the sense that while we
10 are part of the Department of Energy, our funding -- 94% of
11 our dollars come from our customers who are muni's, co-op's,
12 irrigation districts, military bases, national labs, many of
13 whom are small, some of course are big as well.

14 And they are our partners in how we fund all of
15 the activities that we do. Spend roughly 160 million
16 dollars a year on capital, plus numerous other investments.
17 I also want to point out that we take the power from 57
18 hydro-electric dams across the Western United States. Some
19 of the big ones you know, you know, Hoover Dam, Glen Canyon
20 Dam and some very, very small ones.

21 Those dams also provide the grid with very
22 valuable black start capability in addition to the output.
23 When we look at physical and cyber security, it is really at
24 the nexus of where we are, right? Our IT systems are our OT
25 systems integrate much of the western United States with the

1 17,000 miles alignment we have the 320 substations and 485
2 communications sites.

3 So, we take really a three-step approach. We
4 look at both the tactical, the practical and the strategic.
5 From the tactical side for example, in operating technology
6 and how we look at it, we've moved that all into secure
7 enclaves.

8 We've looked at our substations, done 345
9 risk-base assessment on those substations, which ones should
10 we invest in first, what should we do because there's not a
11 one size fits all. We apply a risk-base approach. My
12 nightmare scenario quite candidly is a combined physical and
13 cyberattack.

14 We've seen that in other places and it's one
15 given our footprint. I don't serve the end of the universe,
16 but you can usually see it from one of my substations and
17 that has a real implication and that is for example, we
18 don't have communications out to the edge of the grid very
19 often.

20 And just the nature of having such a diverse
21 system which stretches from Canada all the way down to
22 Mexico from western Minnesota all the way to the Pacific
23 Ocean. So, from a strategic perspective, we also try to
24 figure out how do we make investments over a 10-year window
25 so we can both take advantage of new technologies, but also

1 quite candidly not jack the prices up to our customers in a
2 way that makes it unacceptable?

3 So, there's a very fine, strategic balance we
4 have over a 10-year window. And on a practical basis, we
5 work very diligently trying to see what can we do on
6 substation design? How do we fix the towers in a different
7 way? How do we understand what technologies that we can
8 apply that again doesn't break the bank and at the same time
9 improves our physical and cyber security?

10 I think it's important to recognize as a few of
11 the panelists have, that the threats have many faces and
12 from our perspective, we can't eat the elephant all at once.
13 We have to understand what are the right things to do and
14 what are the right investments.

15 And I can tell you as somebody who's fairly often
16 besieged by the latest, greatest technology, sometimes the
17 best technology is what we have, we just have to deploy it
18 in a different way, we have to understand how to use that
19 data in a different way.

20 I mentioned the secure enclaves -- a perfect
21 example of how to improve the resiliency of our operating
22 technologies. The other piece which is important and that's
23 around regulations. We obviously follow all the CIP
24 requirements and everything that Jim and the team does at
25 NERC, very active with NATF, but at the end of the day I

1 tell my staff it's not just about compliance, it's about
2 the spirit of compliance.

3 It's not understanding what are we actually
4 trying to accomplish, and that's been a mind shift that
5 we've had at WAPA over the last three of four years. It's
6 to understand we're not just trying to check the box and say
7 here we've complied, but rather what can we do to protect
8 and secure our system in a way that helps everyone else?

9 I'll just leave you with the thought, we connect
10 to roughly 100 utilities -- physically connect, I'm not sure
11 even Nick's group connects with that many, and our big
12 threat concern is also though interconnections -- what
13 happens from the very smallest utility that we have to do or
14 the water district, or candidly the military base?

15 That's why we've been so supportive of what we're
16 doing with the Department and defense on the DCEI
17 activities. We look at the 30-some odd military bases that
18 we have in our footprint and do stress that their power
19 supply could be potentially at risk and what can we do to
20 harden the infrastructure for them and at the same time
21 build more resiliency into the entire system.

22 So, thank you so much for hosting this, we really
23 appreciate it.

24 MR. MCCLELLAND: Thank you Mark, Jim?

25 MR. ROBB: Good morning, thank you all for

1 calling this Technical Conference on Grid Security. I'm Jim
2 Robb, I'm about to complete my first lap as the President,
3 CEO of NERC. As Electric Reliability organization for North
4 American I very much appreciate being part of this
5 conversation.

6 I'm sure you all know that there's been no loss
7 of load in North American due to cyber attack and that
8 industry is very committed to security. However, I want to
9 ensure everybody that we know that our work in this area is
10 never going to be over, we'll never rest on our laurels and
11 we will never take comfort in that fact.

12 Our adversaries, as has been pointed out several
13 times today, are persistent, dynamic, determined and growing
14 in sophistication. Electricity supports every aspect of our
15 way of life and well-being. While all sectors of the
16 economy are increasing targets for data theft, ransom-ware
17 and other criminal activity, the electric sector has taken
18 this threat extremely seriously and has put in place I
19 believe, to be a very robust system to protect the critical
20 infrastructure from cyber threat.

21 In recent years we've seen an increase in the
22 sophistication and frequency of cyberattacks. In 2018, the
23 major security trends extended to include phishing, malware,
24 gunfire and theft. Spear phishing, in particular, with
25 credential harvesting objectives remains the most common

1 attack vector because it's so effective and relatively easy
2 to execute.

3 In our work, NERC employs a three-pronged
4 approach to support of the security of the bulk power
5 system. Those three include mandatory and enforceable
6 reliability standards, information sharing, collaboration,
7 and training and drilling. Together they form, we believe a
8 good foundation to effectively confront these ever-evolving
9 threats.

10 Now to be clear, I believe that NERC CIP
11 standards provide a very critical, common foundation for
12 widely recognized essential security practices. I liken
13 them to the CCR's in your homeowner's association. They
14 preserve the value of the neighborhood by ensuring a
15 baseline level of performance.

16 With that being said, I don't think anybody would
17 believe that the standards in and of themselves, are
18 sufficient and it's more important what management and
19 companies do beyond the standards to ensure a completely
20 robust and secure system.

21 So, I'm going to focus my remarks this morning on
22 how those threats are mitigated through NERC's partnerships
23 and the capabilities and the services we're developing in
24 conjunction with industry and government through the
25 Electric Information Sharing and Analysis Center of the EI

1 SAC.

2 The emerging and dynamic nature of malicious
3 cyberthreats requires constant situational awareness, real
4 time communication and prompt emergency response
5 capabilities. That's where robust information sharing
6 programs come in and the EI SAC provides those services
7 on behalf of industry and government.

8 Operated by NERC, working in close collaboration
9 with the Department of Energy and the Electricity Subsector
10 Coordinating Counsel, the EI SAC is the central hub for the
11 sharing of security information within the electricity
12 sector. The EI SAC communicates with more than 1,000
13 companies via a secure portal, sharing critical security
14 information provided by both industry and our government
15 partners. We also conduct periodic webinars, critical
16 broadcast calls and a newly developed all-points bulletin to
17 rapidly inform industry of emerging threats.

18 For example, we issued an all-points bulletin
19 last night regarding the National Defense Authorization
20 Act's identification of the use of certain Chinese
21 technology, particularly at Huawei and ZTE as providing,
22 creating real risk for their systems and wanted to alert
23 industry to that fact.

24 For the most serious threats NERC uses NERC
25 alerts which are used to provide concise actionable security

1 information and mitigation suggestions. NERC alerts are
2 divided into three levels and can require companies to
3 affirm back to NERC that they have successfully mitigated
4 the threat and at the extreme, allow NERC to essentially
5 direct action.

6 Since 2009, NERC's issued 46 security-related
7 alerts, 41 of those were cyber related. In the area of
8 information sharing partnerships, the premiere event in the
9 industry right now is a program we call CRISP, the
10 Cybersecurity Risk Information Sharing Program.

11 Conceived by DOE and managed by the EI SAC in
12 partnership with the Pacific Northwest National Lab, CRISP
13 uses innovative technology developed by DOE in the lab
14 system to monitor cyber activity on company systems. CRISP
15 companies cover more than 75% of U.S. customers. We're
16 working with DOE to expand the program and are exploring
17 integrating data from our Canadian partners.

18 Indicators and threat actor information captured
19 by CRISP is shared beyond the CRISP memberships to all of
20 the EI SAC participant's benefit. Since its inception,
21 CRISP participant costs have declined significantly, and
22 process improvements and experience have allowed the program
23 to rapidly declassify insights for broad communication -- in
24 many cases in less than 24-hours.

25 In conclusion Joe, I was planning to close, but

1 thought I would cite six key challenges that I see ahead of
2 us in this area. These include, first of all, strengthening
3 cross-sector partnerships to facilitate better information
4 sharing and coordination among key interdependent sectors.

5 Second, is developing more advanced and nimble
6 tools to stay ahead of adversaries such as expanding the
7 CRISP-like capability to operating technology area.
8 Securing the electronic devices that are increasingly
9 installed behind the meter, speeding the declassification of
10 critical information, developing a strong cyber aware and
11 cyber capable workforce, and designing the transforming
12 grid in ways that incorporate security concerns upfront.

13 We know that are adversaries are determined and
14 capable, we must remain agile and vigilant and continue to
15 collaborate with each other to share information as quickly
16 and thoroughly as possible. Thank you again for allowing me
17 to speak today, and I look forward to the conversation.

18 MR. MCCLELLAND: Thank you Jim, Tom?

19 MR. GALLOWAY: Chairman, Commissioners,
20 Assistant Secretary Walker, Senior FERC and DOE staff, thank
21 you for inviting me to participate on today's panel. My
22 name is Tom Galloway and I'm the President and CEO of the
23 North American Transmission Forum.

24 The Forum's a voluntary non-profit membership
25 consisting of about 90 transmission companies in the U.S.

1 and Canada, which together in aggregate represent about 90%
2 of the high voltage circuit miles and peak load.

3 The Forum's mission to improve on excellence in
4 the operation of the electric transmission system and we do
5 this by sharing timely and decaded information including
6 best practices, as well as fostering continuous improvement.

7 In 2013, Forum members made the deliberate
8 decision to add resiliency to our mission statement.
9 Reliability resiliency is closely related by different
10 topics. Reliability relates to the transmission system's
11 ability to perform within the defined set of parameters for
12 design-specific contingencies whereas resiliency is the
13 ability to withstand and recover rapidly from severe systems
14 events.

15 We use an all hazards approach through resiliency
16 which includes cyber and physical security and we've divided
17 our focus into three principal areas. Those are to prepare
18 for, to operate through, and recover from significant
19 events. Since 2013, the Forum have jointly run one or more
20 annual resiliency summits on key topics including severe
21 weather and storm hardening resilient system design,
22 security, EMP and GMP threats and cross-sector
23 dependencies.

24 Our next summit is scheduled for next week and
25 will be cohosted this year by NERC and include a number of

1 outside governmental speakers including Joe McClelland from
2 FERC.

3 Beyond conducting summits, we have been an active
4 enhancing member of physical and cyber security in other
5 ways, including developing, maintaining security principles
6 of excellence which go well beyond mandatory compliance,
7 conducting about a dozen peer reviews annually, which
8 includes review of a host member's security performance
9 using those principles of excellence to criteria, assisting
10 members via small focused and highly qualified teams on a
11 range of security topics.

12 Developing best practices and reference documents
13 such as CIP 14 guidance for a determination of critical
14 assets to help our members prioritize physical security
15 activities and conducting webinars on key resiliency and
16 security topics such as key spare parts, incident command
17 structure, substation physical security and planning for
18 resilience.

19 In addition to those routine activities, we've
20 undertaken a number of specific projects along the lines of
21 security. Just to summarize quickly, the first one is
22 supplemental operating strategies, which analyzes the
23 capabilities required to and the strategies necessary to
24 implement manual operation to the grid given a large-scale
25 loss of situational awareness.

1 Our next phase in that project will include a
2 coincident loss of physical assets. The second project is
3 around grid security emergencies and in the event that a
4 grid security emergency is declared, we've been working with
5 the DOE partners to develop a framework to optimize industry
6 response to those orders.

7 And our last project area is around supply chain
8 cybersecurity in response to NERC's CIP requirements, we've
9 been developing a framework within the Transmission Forum
10 and associated criteria so that our members can implement
11 and secure cybersecurity controls around ranges of important
12 equipment including emergency management systems and
13 protective relay.

14 And to kind of underscore what you've heard
15 already today within the Transmission Forum, we consider the
16 top threat to energy infrastructure is the rapid growth and
17 use of digital technology throughout the entire electric
18 system during a timeframe of increasing cyberthreats, the
19 advanced persistent threats by nation states, including
20 threats related to supply chain, delayed sharing of details
21 about those threats from government to industry and
22 laterally throughout the industry due to factors such as
23 limitations and clearances.

24 And lastly, cross-section dependencies in
25 particular communications and fuel and the associated

1 coordination challenges. So, I've included some more
2 detailed write-ups in my written remarks, but I look forward
3 to dialogue as we go forward, thank you.

4 MR. MCCLELLAND: Thank you Tom and around the
5 corner, Don.

6 MR. SANTA: Good morning, my name is Donald
7 Santa. I am the President and CEO of the Interstate Natural
8 Gas Association or INGA. Thank you very much to the
9 Commission, senior officials from the Department of Energy
10 and Transportation Security Administration for the
11 opportunity to speak this morning.

12 The diversity of natural gas end use makes it
13 unique about the nation's energy resources. One of these is
14 generating electricity. The operators of interstate natural
15 gas pipelines appreciate the significant and growing
16 utilization of natural gas to generate electricity, and the
17 resulting effect on the criticality of their infrastructure
18 to the nation's security.

19 The Boards of Directors and senior leadership of
20 INGA's member companies have identified physical and
21 cybersecurity as a top enterprise risk. Last year, INGA's
22 Board of Directors adopted the commitments to pipeline
23 security. This statement emphasizes member company's
24 commitments to first following the TSA Pipeline Security
25 Guidelines.

1 Second, following the NIST cybersecurity
2 framework, and third, engaging in information-sharing across
3 the industry and with our federal partners. This final
4 commitment is important. Strong coordination and
5 cooperation in support of information sharing across the
6 private sector and the federal government is foundational to
7 understanding how best to protect our infrastructure.

8 Risk prioritization begins with understanding the
9 threats. Once we understand the threats, we can determine
10 how to implement security controls that will best deter,
11 delay, respond to and recover from incidents that could
12 result from those threats.

13 Threats are evolving. We now are concerned with
14 the threat from sophisticated, well-resourced nation state
15 actors. We also have seen an increase of domestic threats
16 to our infrastructure from groups who wish to make political
17 statements by damaging our infrastructure or delaying our
18 projects.

19 The emergence of well-resourced determined nation
20 state actors as a principal security threat to the nation's
21 energy system is a threat beyond what the private sector can
22 be expected to confront on its own and goes to the very
23 heart of the role of the federal government in protecting
24 the security of our nation.

25 Pipeline operators rely on our federal partners

1 to share important information about the tactics and
2 techniques used by our adversaries as well as the mitigative
3 measures needed to reduce the risk of a successful attack.

4 In addition to understanding threats, it's
5 important to understand the potential consequences should an
6 attack be successful. The physics of natural gas are
7 completely different than the physics of the bulk electric
8 system. Pipeline operators have means to limit the effects
9 of an incident that are not available to the operators of
10 other energy infrastructure.

11 This is not to say that natural gas pipeline
12 operators take the threat of physical and cybersecurity
13 attacks lightly. The point only is that risk cannot be
14 fully understood without an appreciation of potential
15 consequences.

16 From a legal perspective, the recovery in an
17 interstate natural gas pipeline's maximum rates of the costs
18 prudently incurred to protect physical and cybersecurity is
19 no different from the recovery of other costs that are part
20 of the pipeline's cost of service.

21 A practice impediment to recovery, however, can
22 be whether a pipeline's maximum lawful rate will clear the
23 market. Many pipelines must discount the rates to meet
24 competition, in other cases pipelines have negotiated rates.

25 The Commission's 2001 policy statement on

1 extraordinary expenditures necessary to safeguard national
2 energy supplies provides the flexibility necessary for
3 pipelines to address the unique circumstances in seeking to
4 recover such costs.

5 Affirmation of the continued applicability of the
6 2001 policy statement would be welcomed. The natural gas
7 pipeline operators represented by INGA recognize that the
8 natural gas system is critical to our nation's economy, to
9 the health and welfare of its citizens, and to our national
10 security. An essential element of preparedness to meet
11 security threats is sharing threat information across our
12 industry, across economic sectors and in a robust two-way
13 dialogue with our federal partners.

14 As part of that, pipeline operators are committed
15 to coordinating with our electric industry counterparts as
16 we plan for how to protect this infrastructure from rapidly
17 evolving threats, thank you.

18 MR. MCCLELLAND: Thank you Don, this concludes
19 this part of the panel and I think everyone will be happy to
20 hear it concludes the use of the clock. I'll turn it back
21 over to the Chairman.

22 CHAIRMAN CHATTERJEE: Thank you Joe. Yes, that
23 concludes the use of the clock, but I am cognizant that
24 we've got an hour and five minutes to get through a number
25 of questions, so we'll try and limit ourselves to about 10

1 minutes each. Thank you all for those fantastic
2 presentations, very, very informative.

3 I want to start you know, ADP has been a real
4 leader in cybersecurity and my understanding is that you
5 made a strategic priority -- sorry, it doesn't count against
6 my time. I understand you made it a strategic priority to
7 strive for cybersecurity excellence above and beyond the
8 requirements of NERC CIP, so Nick, if -- as your company
9 thinks about cybersecurity, can you kind of elaborate what
10 guides your thinking on where and how to expand your limited
11 resources?

12 MR. AKINS: Yeah, absolutely. You know we
13 actually -- cyber, meet with a regular basis with the CEO
14 and the Board, and we also participate in drills together
15 from a cyber perspective, from a business continuity
16 standpoint.

17 And the reason for that is really pretty simple.
18 I mean it not only goes to compliance, it goes to
19 operational excellence and if your brand is built around
20 operational excellence and you see it as a really something
21 that can really diminish the brand, there's nothing worse
22 that could happen to a company in our opinion to have a
23 significant outage caused by any event, but let alone a
24 cyber event.

25 So, it really is not only a defensive posture,

1 but also offensive to ensure that we enable that brand to
2 equity. And so, in our relationships with the government is
3 really critical in that and we've established very credible
4 relationships, ongoing real time relationships with our
5 staff along with the various parts of the government and
6 with NERC.

7 And also, we take it very seriously to
8 participate in the Grid X exercises. There's nothing better
9 for this industry than drills of all different types and the
10 Grid X exercises are probably some of the first and I've
11 probably participated in almost all of the grid X exercises
12 because of the importance, not only to our company and the
13 Board, but also importance to that culture that says that
14 we're going to continue to advance that in a very positive
15 sense.

16 CHAIRMAN CHATTERJEE: Thank you. As you all know
17 I've been very focal about my concern regarding the security
18 of gas pipelines and the impact that the loss of pipeline
19 could have on the electric grid. As Commissioner Glick
20 mentioned, several months ago GAO came out with a report.

21 It was pretty critical of TSA oversight of
22 pipeline security. Miss Proctor, I was hoping you could
23 talk a little bit about TSA's response to that report and
24 whether it's changed the way you assess potential threats
25 and vulnerabilities on pipelines?

1 MS. PROCTOR: Yes, Mr. Chairman, we certainly did
2 review those concerns and we believe that TSA has both the
3 tools and the authority to address any threats within the
4 pipeline industry.

5 From a tool perspective, we've talked about the
6 Pipeline Security Guidelines, and as guidelines, they
7 provide us the flexibility to address threats outside of the
8 time-consuming regulatory process which could conceivably
9 take months or even years to go through.

10 Using the Pipeline Security Guidelines, we can
11 meet with industry and identify those concerns and threats,
12 work with industry to find the best mitigating measures to
13 incorporate in the Pipeline Security Guidelines.

14 However, in the event of a significant or
15 imminent threat, Administrator Pecoske has the authority
16 today to issue a security directive to specifically address
17 that threat and to require specific actions on the part of
18 the pipeline industry and those actions -- that security
19 directive, would have the force of a regulation.

20 And that regulation would remain in place for the
21 duration of the threat and the pipeline industry members
22 would be required to comply with that to address any
23 existing threat. We believe that that provides us with both
24 the tools and the authority to be able to address any threat
25 situation.

1 The primary way that we address threats is what's
2 been referenced here in some of the comments you heard this
3 morning and that's with information. And that's making sure
4 that our pipeline industry partners are getting the
5 information, getting the briefs, whether it is classified
6 information or otherwise, so that they're aware of the
7 threat and can take those mitigating actions to offset that
8 threat.

9 So, we believe between informing and educating
10 our partners about the threat, having the flexibility to
11 incorporate new mitigating measures with the input of the
12 industry and our government partners, and in the case of
13 that imminent threat, having the administrator to issue, if
14 necessary, a security directive that would have the force of
15 a regulation. We believe that that would address the
16 threat.

17 CHAIRMAN CHATTERJEE: Thank you, that's very
18 helpful and I'm glad to hear about all that good work. As a
19 related follow-up question, because there are no mandatory
20 security standards for gas pipelines, it's obviously very
21 important that entities are willing to engage on a voluntary
22 basis with TSA and its federal partners like DHS and FERC.

23 Do you feel like industry is stepping up to the
24 challenge and engaging voluntarily? The reason I ask is
25 because I've stated a number of times that TSA and industry

1 should have an opportunity to better address cybersecurity
2 concerns on a voluntary basis before anyone imposes
3 mandatory cybersecurity standards for gas pipelines.

4 So, I'm just interested in your view on whether
5 industry is taking advantage of the opportunity to engage
6 voluntarily?

7 MS. PROCTOR: Mr. Chairman, I do believe that
8 they are as I mentioned in my opening comments. Our first
9 cyber architecture reviews were with your agency and
10 Director McClelland's team and we conducted seven of those.
11 Those were voluntary, so there was voluntary participation
12 by our pipeline security partners and now we've moved into
13 the second phase of these cybersecurity reviews.

14 The validated architecture design reviews that
15 are being conducted by CISA, the Cybersecurity
16 Infrastructure Security Agency, so, we're in the process of
17 conducting those reviews with them. Now, we've started that
18 process and certainly some of the companies have indicated
19 that they wanted to see how those reviews went with some of
20 the others.

21 With the review that's been done so far, we've
22 had very good feedback from the CEO of the company. I think
23 he's an advocate for the cybersecurity reviews now. So, we
24 are in the process now of scheduling at least four other
25 additional reviews at this point.

1 So, we do expect that we're going to have a full
2 schedule of reviews as we committed to.

3 CHAIRMAN CHATTERJEE: That's very, very good to
4 know, thank you. One thing I said on a number of occasions
5 is that we can't necessarily design the grid to protect
6 against every single threat out there. There are just
7 simply too many quickly evolving threats and designing the
8 grid to withstand every permutation of threat would just be
9 cost-prohibitive.

10 So, I'd just be curious for the panel's thoughts
11 on what types of mitigation measures provide the best bang
12 for your buck in terms of cost effectiveness for both
13 physical and cyberthreats? Anyone, yeah you can start.

14 MR. AKINS: So, first of all as we go through the
15 process of identifying critical facilities and the real
16 issue is to get as many of those critical facilities off
17 that list as you can. And we've made a lot of progress in
18 terms of reducing that component, but because of the various
19 features we put in place.

20 The main thing you'll see across the board
21 though, we're putting in our own private fiberoptic network
22 for example, for communications, hardening the facilities,
23 designing and spec'ing for those things. One of the best
24 things we can do though is SCATA and top acquisition from
25 various points of the system. You'd be surprised how low

1 the percentage is of actual SCATA status of various parts of
2 our system that we see, and we continually invest to raise
3 that level.

4 And now you're seeing monitoring devices that
5 aren't even attached to the SCATA system, so you're able to
6 do a lot more things today than what you have been able to
7 do in the past. And that's the biggest thing for the buck
8 right there in terms of visualization, analytics going on in
9 the background, and the ability to really focus on different
10 parts of the system and being able to not only look at the
11 present status, but also response characteristics.

12 CHAIRMAN CHATTERJEE: I just wanted -- Mark do
13 you want to weigh in on it?

14 MR. GABRIEL: Sure, some of it is relatively
15 simple in design change. When we do something like no cut,
16 no climb fencing right, where the story is you can't get a
17 cowboy boot in it right? And I know that sounds simple, but
18 there's some real nuts and bolts things that we have to do.

19 Changing the lock systems. Many substations are
20 shared across the United States, and very often there's
21 multiple people with multiple keys and multiple locks -- so,
22 that's on the one side.

23 I agree 100% with Nick, the more we can do with
24 SCATA, and fiber around that, the better off we're going to
25 be and information sharing -- I think you've heard that as a

1 common theme, I continue to be concerned on a daily basis
2 that we're dealing with something that moves at the speed of
3 light and then we're moving at the speed of email, and those
4 two things are not necessarily compatible.

5 We may not see an incident going on, we could
6 share -- we've had instances where substations are literally
7 next to each other, different owners, if something happens
8 at substation A, we don't hear about it even though
9 substation B is literally 100 yards away.

10 So, the simplest thing from my perspective is get
11 real time information as quickly as we possibly can.

12 CHAIRMAN CHATTERJEE: In that vein, since we
13 can't guarantee it will stop every threat actor every time,
14 we have to prepare with a recovery plan so we can try and
15 restore service to customers as quickly as possible.

16 So, Mr. Galloway, I know the NERC standards had a
17 baseline in terms of requiring a CIP recovery plan, and
18 having things like a black start plan, but the standards
19 don't necessarily cover all the issues that could arise
20 following a physical or cyberattack.

21 Are there aspects of recovery that you think the
22 industry should be paying greater attention to? And is
23 there any way that FERC can help place more of an emphasis
24 on those issues?

25 MR. GALLOWAY: So, thank you for that question

1 Chairman. So, we have been spending a fair amount of time
2 over the last couple of years on recovery best practices and
3 really kind of looking at from agnostic from the causation,
4 right?

5 So, if you just premise that you have a
6 wide-scale outage, you know, what do you have to do in terms
7 of communication with others cross sector-wise and so forth
8 in kind of promoting those relationships in that kind of
9 activity?

10 So, a number of our members have now evolved to
11 do annual drills that kind of augment the Grid X exercise
12 that's run by NERC. One in particular, is like a resilient
13 grid exercise over the last five years that now features a
14 physical and a cyber component and is part of the causation
15 and really kind of has a whole of community response in
16 terms of a connection between the industry and the
17 governmental partners, both state, local and federal.

18 So, we've really been emphasizing that. We have
19 stood up a new project around black start, making sure that
20 there's sufficient diversity, numbers of black starts in
21 situationally placed to be advantageous on the system.

22 With respect to that, I certainly welcome a you
23 know, a continued dialogue with FERC and others on how we
24 could progress on those fronts.

25 CHAIRMAN CHATTERJEE: Thank you for that. I want

1 to be sensitive to my colleague's time, so just one final
2 follow-up, Mr. Galloway, I noticed in your prepared
3 testimony it's very interesting at the end you noted that it
4 would be helpful if the federal government could ease
5 barriers to transporting large transformers.

6 Good news today is we've got some people here who
7 know a few things about transportation, and I was just
8 wondering if you could elaborate on what those barriers
9 might be and what could be done to help address those
10 barriers?

11 MR. GALLOWAY: So, you know, there has been a
12 lot of industry focus in terms of key spare parts, in
13 particular, large power transformers, and so EEI's done a
14 lot of great work in terms of the identification of the, you
15 know, the subset of those items that were most critical.

16 One of the areas that has been an outflow of that
17 is the transportation -- pardon me, transformer
18 transportation working group that's run by EEI and they've
19 identified kind of a range of challenges in terms of
20 permitting, you know, for interstate communication of the
21 equipment, both from a procedural standpoint and from a
22 physical standpoint -- can the roadways, can the bridge and
23 so forth kind of accommodate transport in these loads, large
24 loads in a finite period of time.

25 So, I think that that's progressed quite a bit.

1 I think there's still some residual challenges there that it
2 might be helpful to get FERC interaction on the front to
3 help smooth those out.

4 CHAIRMAN CHATTERJEE: Thank you, just one final
5 thing. My colleague, Commissioner Glick, who still
6 maintains the outstanding Senate staffer skills that he had
7 pointed out that Nick you were going to weigh-in on the last
8 question I was asking, sorry.

9 MR. AKINS: It sort of ties into this question
10 too and he brought up the spare parts programs. We have
11 several spare parts programs, EEI, grid assurance, all those
12 and really if we can marshal the spare parts and we have
13 consistency among the grid itself, it will be a tremendous
14 value and we can work with the transportation partners to
15 locate the spare parts in areas of the country that we can
16 mitigate the impact from a transportation perspective.

17 So, those are things that we continue to work on.
18 The other is you know, after super storm Sandy, we did a lot
19 to merge the regional response networks associated with
20 recovery aspects. We're also patterning that into cyber
21 mutual assistance as well among the industry participants.

22 So, that work is continuing too, to try to
23 mitigate the impact of all this.

24 CHAIRMAN CHATTERJEE: Thank you, I'm going to
25 file closure on myself and yield the floor to Secretary

1 Walker.

2 MR. WALKER: Thank you Chairman. So, one of the
3 challenges I think we've heard as we continue down the path
4 working with our organizations in the Department of Energy
5 as well as within the Office of Electricity is the
6 challenges associated with accurately capturing how fast the
7 industry is moving from a solutions-set, specifically as it
8 relates to cyber.

9 So, computer technology changes roughly every 60
10 days and our ability to obviously keep up with that doesn't
11 necessarily match the recovery mechanisms for remuneration
12 in the industry whether it's from a regulatory model or from
13 a PMA model or from just a pure for-profit business.

14 So, what are the things -- and Nick, I'll address
15 this to you and Donald to you and Mark you can weigh-in as
16 well, I think. What are the things that we should be
17 looking at that enable us to be able to capture what are
18 those best technologies to ensure that we can, you know,
19 roll them through -- I know cloud technology is another one
20 where in some jurisdictions we're talking about capitalizing
21 others at OEM expense, and I know the regulatory models make
22 it a little bit more challenging when it's known expense
23 versus a capitalized cost.

24 So, I'd like your opinion on that because that's
25 one of the biggest challenges we see in the industry. Nick,

1 maybe you could start?

2 MR. AKINS: Sure. So, yes, it is an issue but
3 really, we found our state commissions are supportive of the
4 aspects. As a matter of fact, we have some cyber riders for
5 recovery to try to bring the costs of cyber-related costs
6 closer to the recovery aspect so the OEM part of it doesn't
7 hit us so hard. And the other thing too is, we run over a
8 hundred different tools on our system, whether off the
9 shelve, whether developed on our own or whether your tools
10 from the government perspective, and I think those kinds of
11 opportunities really enable us to take advantage of scale so
12 that we're as efficient as possible in that regard.

13 So, as long as we really feel like we're doing
14 the right thing and can explain on a regular basis with our
15 commissions, we're in pretty good shape from that
16 perspective. You know, typically we won't get disallowed a
17 cost associated with resiliency and reliability of the grid
18 and that's really probably one of our least risky
19 investments we can make.

20 MR. GABRIEL: Well, from our perspective, we've
21 got a slightly different financial challenge. We have the
22 same challenge as everybody trying to figure out gee, what's
23 the latest and greatest, what's the next thing that's going
24 to be hitting us.

25 Our legislative mandate is to be the lowest

1 possible cost consistent with sound business principles. Of
2 course, our customers hear the lowest possible cost part and
3 not the consistently sound business principles. And so,
4 it's sometimes a challenge to get funding for things that
5 help the grid at large, as opposed to the smallest customer
6 that we have.

7 But from a technology perspective, it requires
8 continual diligence. We've got a limited staff on our IT
9 and cyber space, they focus day in and day out to understand
10 what are the changes in technologies, what can we do to
11 understand what those implications are, and let's face it,
12 the big issue that we all face is the biggest risk from my
13 perspective to the grid and to the IT space are the
14 individuals that we have working, who either wittingly or
15 unwittingly expose us every single day to risk.

16 So, for us that means lots of training, repeated
17 training, repeated testing, and trying to work through the
18 system. Work the folks to understand that they are the weak
19 link in the system.

20 MR. AKINS: Bruce, if I could just follow-up
21 real-quick too. One of the challenges in the industry is
22 you know, the smaller operating companies in the industry
23 certainly have a challenge from that perspective because
24 they don't have the wherewithal to be able to invest in all
25 these kinds of activities that the larger companies are and

1 we're only as good as our lowest common denominator, so we
2 really have to find ways of insuring that the industry moves
3 forward together from that perspective, and that's where,
4 you know, obviously we as partners can have a big, big
5 process in that to make sure it happens.

6 And we've done that with CRISP and other type of
7 activities.

8 MR. SANTA: You know for interstate natural gas
9 pipelines, while the pipelines are regulated on a cost of
10 service model, in the market there is competition. And so,
11 the fact as I noted in my remarks that pipelines often have
12 to discount their rates, and in many cases negotiate those
13 rates, there's not a legal impediment to recovery of these
14 costs, but I think there is a practical market impediment.

15 Having said that, nonetheless, you know, the
16 pipeline operators, this is a top priority. This is an
17 enterprise risk. The dollars are going to be spent
18 regardless of whether or not there's a guarantee of cost
19 recovery.

20 So, I think from the perspective of what can the
21 federal government do, how can we take advantage of whether
22 it's research and development, whether it is information
23 sharing, other things that the federal government due to the
24 scale, due to the resources it can bring to bear, that we
25 can benefit from that and then have the ability of pipeline

1 operators to adopt that.

2 MR. WALKER: And as a follow-up Donald, one of
3 the things I think today most people would acknowledge that
4 natural gas pipelines play a more important role than they
5 ever have in the past, so if I go back 10-15 years, 10% of
6 the electric generation was provided through natural gas
7 pipelines.

8 Today we're in the 30 to 35% range, and I know
9 from sitting down with Jim Robb's team, that's seemingly
10 going -- that number's going up. That, sitting in the
11 Office of Electricity, makes me very uncomfortable.

12 What are the things that number one, you
13 mentioned earlier that they operate -- your operators
14 operate the system differently than the bulk power system
15 from a being able to you know, avoid cascading events, and
16 things of that nature.

17 So, one I'd like you to illuminate what are some
18 of those differences, and are we at the federal government,
19 particularly through R&D and from the tools that we can
20 provide, that I know we've spent a lot of time on the
21 electricity side taking a look at -- where can we accelerate
22 our efforts in oil and natural gas so that you know, there's
23 100% parity between the two and particularly as we -- the
24 inter-dependent's become that close?

25 MR. SANTA: You are correct. I mean I think part

1 of the -- one of the results of our natural gas abundance
2 and the affordability of it in a number of other attributes,
3 it's used a lot more in electric generation, used a lot more
4 in our economy. We are well aware of that and therefore the
5 increased utilization and the criticality of the facilities
6 operated by our members.

7 In terms of those differences, I mean it could be
8 summed up as simple as this -- electricity moves at the
9 speed of light, natural gas through a transmission pipeline
10 moves at 10 to 20 miles per hour.

11 So, there is the ability and therefore the
12 system, unlike electricity, does not need to be balanced
13 instantaneously. As a result of that, there is time to
14 respond should there be a disruption. In addition to that,
15 the operators of pipelines have a number of means necessary
16 to address this.

17 They can isolate the segment of pipe where
18 there's a disruption. In many cases they can reroute
19 natural gas. They could take advantage of the diversity of
20 supply sources and storage locations.

21 In addition, I think it's important to recognize
22 that the administrators spoke about the fact that security
23 and safety are kind of flip sides of the same coin. And so,
24 some of the very design features and processes that we have
25 as a result of PHMSA safety regulations also are a benefit

1 here.

2 Whether it's the fact that for example mechanical
3 pressure release valves will operate, you know, regardless
4 of what's going on on the SCATA side.

5 The fact that pursuant to the PHMSA regulations,
6 pipeline operators are required once a year to operate their
7 systems mechanically without the SCATA. And that's an
8 important plight because while obviously we separate our
9 commercial systems from our operational systems, if you made
10 the assumption that the SCATA was penetrated, the ability of
11 pipeline operators to operate the system manually, the fact
12 that a lot of the safety features designed to protect the
13 public also protect security I think should be taken into
14 account..

15 On the third part of your question, I think we
16 should look at you know, what has the Department and other
17 agencies done with regard to the electric sector that maybe
18 is transferrable to gas? For example, I know that one of
19 our member companies has expressed interest in learning more
20 about CRISP. So, what can we do to accelerate that, see to
21 what extent it could be applicable to our sector?

22 MR. WALKER: Great and building off of something
23 that Jim had mentioned before, particularly with the notice
24 that went out through NERC and, thank you very much Jim, for
25 that, you and Bill.

1 One of the things I haven't heard a lot of this
2 morning is the reliance of both running the oil natural gas
3 as well as the electricity system, the reliance on the comm
4 structure -- the communication platform. And when you look
5 at things like cybersecurity vulnerabilities, obviously that
6 presents sort of challenges onto itself which is why Jim,
7 you guys sent out that TPL yesterday afternoon.

8 And so, what are the efforts that are being
9 undertaken and Tom, I'll push this to you with regard to the
10 transmission system, particularly given some of the optical
11 ground wire capabilities that exist on the transmission
12 system, and maybe that's an area where we can strengthen and
13 really put some effort into creating a ubiquitous fiber
14 optics network throughout the country, so that maybe Nick
15 you can jump in too and I know you have some in your system
16 and Mark as well, but Tom?

17 MR. GALLOWAY: Yeah, thank you Assistant
18 Secretary. The -- communications is one of the key
19 interdependencies that we're looking at, so I referenced
20 earlier the project that we put together on supplemental
21 operating strategies. And that was one of the prime
22 findings from that effort is that interruption of
23 communications -- voice and digital, was like the top
24 capability that the team came up with in terms of the things
25 that you had to compensate for in terms of operating the

1 system manually.

2 So, that project really kind of envisions
3 interruptions in that way and then how would you work
4 around, you know, around that case? We've continued to
5 highlight the importance of communications in terms of
6 restoration activities in the drills that are members are
7 involved in, and most recently we've signed an MOU with a
8 like corporation called UPC that's involved in
9 telecommunication space to see if we could kind of merge our
10 efforts there and work towards kind of the vision that
11 you've just articulated which is a very robust communication
12 systems that would withstand and be there, you know, post
13 event.

14 MR. WALKER: Nick?

15 MR. AKINS: Yeah Bruce, so first of all fiber
16 optic cable obviously is being placed in substation
17 environments and from an overall communication standpoint,
18 also monitoring methods are changing dramatically as well,
19 so we're going to have other avenues for monitoring.

20 We're also hardening the telecommunication sales,
21 you have that and you have the ground cables being hardened,
22 and so from a communication standpoint it at least gives
23 more solid communications where you don't have fiber optic
24 capability. So, but the focus is to put as much fiber optic
25 in as we can, and that will continue throughout -- probably

1 through the industry because you've recognized that that's
2 obviously a significant dependence of ours.

3 We're also working on with the telecommunications
4 industry on technologies that they're deploying, you know,
5 the regional satellite structures and those kinds of things
6 that we -- that actually are supporting us in ordinary
7 recovery efforts and that could be an opportunity as well.

8 So, we look at all of that in the context of
9 those communications aspects. That being said though,
10 there's also work being done on okay, what if communication
11 isn't there and as long as the substations are operable,
12 which that's why you have all the hardening and all those
13 kinds of activities, we can put people at substations and we
14 could put people at generating stations and monitor
15 frequencies and run the system.

16 Now, there's you know, retirees that we'll
17 probably have to bring back to help us do it, but it could
18 be done, and it could be done in an islanded fashion if it
19 came to it, but certainly we're trying to avoid that with
20 the other telecommunications opportunities we've got.

21 MR. WALKER: Great thanks.

22 MR. GABRIEL: Yeah, I would agree too, the fiber
23 component is critical. We've got roughly 5500 miles of our
24 17,000 miles of line with fiber and of course everything we
25 build today has the fiber on it, and bridging that gap is

1 one of the challenges and the opportunities.

2 I also think what we do on our microwave sites --
3 again 485 different communication spots, but here's the
4 challenges. We learned in the car fire in California, back
5 last summer where we lost -- we went to an N Minus 15
6 condition, lost 15 transmission lines in 8 substations.
7 Fiber optic doesn't burn but the rubber or the coating melts
8 and the fiber breaks.

9 So, and at the same time when you've got a
10 wildfire situation, satellite phones don't work because of
11 the activities and all the dust and ash in the sky. So,
12 what we're looking at thanks to some of the work in the
13 department is what are the alternative technologies that we
14 can use?

15 For us it's about having multiple ways to
16 communicate, multiple ways to look at things, whether it's
17 fiber, microwave, alternative radials, and it's something
18 that we learned the hard way in the car fire, what you have
19 to do, especially when you're sending men and women out into
20 a fire zone to keep power on or restore power.

21 MR. WALKER: Great, thank you, Chairman?

22 CHAIRMAN CHATTERJEE: Thank you Secretary Walker.
23 Administrator, the floor is yours.

24 MR. PEKOSKE: Okay, thank you Chairman. Thanks
25 everybody for your comments this morning. I've just got

1 really probably two or three key questions and really for
2 any member of the panel to address. But I think all of us
3 are in the risk management business. I mean that's what we
4 do. I think every single panelist has mentioned risk
5 management along the way.

6 We have a very significant risk assessment and
7 risk management process within TSA, but I always ask myself
8 the question -- am I best of class in risk management? Is
9 there something that I might be missing in my own risk
10 management process?

11 What I'd like to get a sense from all of you is
12 how do you feel about your overall risk assessment/risk
13 management process and do you feel that there's enough best
14 practice interchanged amongst you?

15 Because I will tell you that you know, from where
16 I sit as I mentioned, government has some pretty
17 sophisticated systems, but I think the private industry has
18 some very sophisticated systems too and might bring up some
19 characteristics that we may discount.

20 And then the follow-on piece to this is how
21 comfortable are you that partners are assessing and managing
22 risk with roughly the same priorities that you are? I mean
23 as you're dealing with federal partners, state partners, I
24 would you know, think it would be pretty frustrating if you
25 thought risk was way over here and your partners were

1 somewhere in the middle of the scale potentially.

2 So, just to kind of give me an assessment of how
3 you feel about your own process, how you feel about the
4 exchange of best practice and then how you feel about
5 alignment of risk, where that alignment is critical?

6 MR. AKINS: It's more like cyber, if you answer
7 yes and yes to either one of those questions it's a bad
8 thing, right? So, I believe that we're doing better. I've
9 been involved with the Electric Subsector Boarding Council
10 since the beginning, like 6 years ago and the way that the
11 federal agencies are working with us today in the industry I
12 think is just very, very good.

13 We're growing together, we're learning together.
14 The grid X exercises certainly have been a key component for
15 sort of step changes in terms of the things we just I mean,
16 like car fires and stuff like that, I mean things that may
17 happen, they'll have an impact.

18 I think we're doing a much better job of that,
19 but I think also we're moving to the next stage of
20 development and that's the analytics, and the execution
21 around it. We're doing much better at that in combination
22 with our government partners, so I believe that you know,
23 we're behind the curve, but we're catching up.

24 MR. GALLOWAY: The -- from a process standpoint
25 we have a practice group of our members that's focused on

1 developing best practices around risk assessment control, so
2 that group will come together periodically and kind of talk
3 about what our individual members have implemented, kind of
4 what's best in class among the members and then those areas
5 that there appear to be gaps that we'll set up teams to kind
6 of fill those gaps.

7 So, I think that that's kind of a word in
8 progress. We started that kind of centered around NERC
9 compliance, but we've broadened it out to be more kind of
10 enterprise-level risks, you know, in terms of the scope of
11 that effort.

12 In terms of kind of connectivity and alignment
13 with others, in terms of the perceived risk, I would echo
14 Nick's point. I think we've grown the relationships between
15 the government and the various sectors, you know, we're just
16 learning from one another and I think there is good and
17 improving alignment on that front, but a lot of it is really
18 kind of knitting together those opportunities to kind of
19 interact and kind of share perspectives and recalibrate
20 based on that.

21 MR. KOSAK: So, sir I don't think anything I say
22 will come as a surprise to you and it sort of gets to the
23 Chairman's point about can you prioritize anything, you
24 prioritize nothing, and Commissioner LaFleur also mentioned
25 the complexity of the stakeholders across just the federal

1 government, much less out to the broader community of
2 interest.

3 For me I think we're getting better as well. I
4 feel like we're at a good place right now, particularly
5 through the leadership, you know, Bruce Walker has
6 demonstrated as well as others at DHS. It's interesting,
7 you do have stovepipes in any organization, right? So, you
8 have the intel community, they're fantastic. They know a
9 lot, they learn a lot, they're very protective of sources
10 and methods.

11 You have the law enforcement community, they know
12 a lot, they learn a lot, they're very focused on prosecution
13 and discovery. And then you have the operator community who
14 are expected to execute when the time comes.

15 And so, I think it's essential, in fact we're
16 getting the combatant commands together increasingly. I'll
17 be at NORTHCOM next week, bringing the Deputy Commanders of
18 STRATCOM, of NORTHCOM, CYBERCOM as well as TRANSCOM together
19 and we see this as being a huge responsibility.

20 The ability for -- and you heard, you know,
21 Chairman General Dunford say before the staff the other day
22 the ability to deter some of these things -- the indications
23 and the warnings are very complex.

24 We're leaning forward in terms of not only just
25 defending ourselves, protecting ourselves, but also looking

1 to defend forward as a means of addressing the threat. But
2 when you think about just within DOD, such a complex entity,
3 you have the asset owners who are the services, and then you
4 have the mission owners who are the combatant commands, and
5 we have a government structure within DOD that is co-chaired
6 by the Office of the Secretary of Defense and the Joint
7 Staff and we're bringing the asset owners and mission
8 owners together.

9 The mission owners are becoming more cognizant of
10 the vulnerabilities of their own plants, particularly as it
11 relates to our ability to flow forces within the United
12 States and our ability to project power to build lethality
13 abroad.

14 Nothing's perfect, but through their cognizance
15 and vulnerabilities affecting their executability and then
16 they're interfaced with the services who own and manage
17 those assets, that is leading to a lot of planning going on
18 to try to get around some of these expected, or problems we
19 anticipate and make investments internal to DOD.

20 But also, just working with Bruce Walker,
21 information sharing. That's the absolute critical piece as
22 everyone on the panel has been saying that we've got to get
23 better, we've got to get better real time to be able to get
24 ahead of the threat, not just observe and react, but be
25 really anticipatory.

1 Because as we move towards artificial
2 intelligence and quantum computing and you know, machine
3 learning and big data, the fact of the matter is that these
4 are consequential and probable attacks.

5 For Commissioner LaFleur, she mentioned EMP for
6 example. So, that's a high consequence, lower probability
7 type of event for which we will be very discerning as to
8 where we harden. Real defense critical missions, you know,
9 nuclear command and control and communication, so we can
10 convince our partners within the government and without to
11 the interagency and to industry that we're really focused on
12 those critical pieces to defend the homeland and protect the
13 American people.

14 For these more, for these in some ways, equally
15 consequential, more probable events, that's where we really
16 need to delineate and really slice and dice and get to a
17 place where we know we can't plan around something, and we
18 know that if this particular asset comes down as a result of
19 an attack through an industrial control system or some other
20 type of physical or cyberattack that multiple load plans
21 will fail.

22 And our ability to do our job, the ability of the
23 Secretary of Defense to do his job, his essential functions
24 would be impacted. So, the bottom line upfront to your
25 question is team DOD is always working to be better. I

1 think we're in a better place than we were you know, 10
2 years ago, 5 years ago, but I think given what you've heard
3 from my colleague from the DNI today, the threat is here and
4 now, and the threat is growing very sophisticated.

5 And the likelihood that we're going to face this,
6 it's not a question of if this is going to happen, it's
7 going to happen. The question is what are we doing to
8 mitigate it, and what are we doing to be able to deter our
9 adversaries from being able to do it in the first instance?

10 MR. PEKOSKE: Sure, and all that goes to
11 allocation of resources and effort and that's sort of the
12 focus of my question, yes sir?

13 MR. GABRIEL: You know, I think as an industry
14 and certainly as our organization, we're getting better at
15 what I'll call the mechanics of risk -- the FCC work we've
16 done, other work across the industry.

17 Where I get a little bit concerned is on sort of
18 the fringes. For example, we've talked about black start.
19 Well, it's one thing, every -- we all have black start
20 plans, but how they have been or not been coordinated with
21 the states for example, we worked with the Governor of
22 Wyoming last year because we found that our plans were
23 mitigating our risk as an operator, but they weren't fitting
24 the risks that the state felt that they have.

25 The same thing in certain markets for black

1 start, you can't bid in black start units from hydro, which
2 are the best, in my opinion, black start units because low
3 cost natural gas units are bidding in for black start.

4 Well that works just great for risk mitigation as
5 long as there's not a pipeline freeze over, right? So, it's
6 an interesting dynamic. As I said we can get to the risk
7 from our edge so to speak or where I may need Nick's system,
8 but then how does it go to that next level because what I
9 see as a huge risk may not be the same thing that the states
10 see or that a market may see.

11 So, trying to get some more clarity around that I
12 think would be a great idea.

13 MR. SANTA: I'll at least address it briefly from
14 the gas pipeline perspective. And I think this echoes a lot
15 of what the -- my colleagues from the electric power
16 industry have said. I think that on risk management we are
17 doing better, improving. We still have a long way to go to
18 get even better, but I think there clearly is the dedication
19 to it.

20 We benefit from collaborative exercises, whether
21 it's within the INGA Physical and Cybersecurity Committee,
22 the oil and gas sector, Subsector Coordinating Council, the
23 fact that we're now beginning to participate in ESCC
24 meetings. As a matter of fact, at that meeting that
25 occurred just recently, several members from our new Chief

1 Information Officer Task Force participated in that
2 meeting.

3 And also, Mr. Akins has mentioned the grid X
4 exercise. And that exercise, we have been working very
5 closely in terms of developing scenarios that will involve
6 natural gas and also encouraging our member companies to
7 participate in that.

8 I think that the information sharing with our
9 federal partners is key and is critical. That is an area in
10 which there has been a lot of improvement, but I think there
11 still is a way to go there and I think certainly in terms of
12 is certain information over-classified? That should be
13 looked at, and also quite frankly just something as simple
14 as security clearances, to make sure that those within our
15 member companies have the clearances to be able to have
16 access to that information.

17 MR. ATKINS: If I could just jump in with a quick
18 comment. Mark brought this up -- black start capability.
19 This coordination that's going on today is nothing like, I
20 mean it's much better than it has been ever in the past.
21 And we're seeing commonalities that we can actually manage
22 risk together in many respects and black start for example,
23 placing our black start facilities near military
24 facilities, not only helps with that mission, but also helps
25 with our societal mission around the ability to bring the

1 grid back.

2 We talked about the spare parts, to work with
3 your agency on transportation options associated with that
4 particularly in the event of recovery, is an extremely
5 positive event that can occur that mitigates costs for
6 everyone and mitigates risk. So, I think the level of
7 discussion that's going on today through these exercises and
8 others are bringing up multitudes of questions for us that
9 we're working together on.

10 MR. PEKOSKE: Okay, thank you and the other
11 question I have concerns the standards process. A number of
12 you said that the standard setting process disclosed,
13 certainly in cybersecurity it's probably by definition
14 always going to be slow given the speed at which that moves.

15 What would your recommendations be for an
16 improvement in the cycle time for standard setting? And
17 then to the extent that that would not be satisfactory, how
18 do you address having some baseline level of performance?

19 MR. ROBB: I guess that probably comes my way.
20 You know, I think our standard setting process gets a little
21 bit of a bad rap. It doesn't move at the speed of sound,
22 that's for sure and if something doesn't move at the speed
23 of this risk, which is one of the reasons why a standard
24 can't be the solution to every problem, right?

25 The standards that we have in place as I said

1 really kind of set that baseline foundational level to be
2 robust against any kind of an event as opposed to a specific
3 event which is what you would be chasing if you were trying
4 to standardize your way out of every threat.

5 The one thing that is effective about the NERC
6 standards is that they're developed through a very rigorous
7 process, it's highly participative, it's highly
8 consultative. It does take a while, but the good thing is
9 once the standard is done it's not contested, right?

10 By the time it comes to FERC right, it's -- you
11 don't have litigation around it and so forth. Whereas,
12 opposed to government regulation or something like that
13 where, you know, there typically is litigation. So, I think
14 our ability to actually move from need to actionable
15 standard, if you look at the full cycle time, it isn't that
16 bad.

17 We have moved some along very, very quickly, but
18 again I don't disagree with the basic notion that it's a
19 cumbersome process and has its issues. I do think the
20 important thing to think about from my advantage and
21 experience here is to be fairly thoughtful about what you're
22 trying to put standards around and what you're not because I
23 think everyone would agree the standard is a solution to
24 many problems but certainly not every problem.

25 MR. GALLOWAY: Can I add in on that? So, you

1 know, one of the things that we try to do and it's probably
2 highlighted in the security area, is try to be that much
3 more agile so as risks do emerge, we'll put together
4 principles of excellence that we can stand up in a pretty
5 rapid fashion -- you know, certainly less than a year, you
6 know, for most topics.

7 So, we work closely with NERC and with FERC now
8 more recently on what they view as risks in this domain and
9 we use that as inputs into our decision-making process in
10 what the next iteration of principles of excellence should
11 be.

12 So, then we'll start to deploy those out through
13 the membership through our peer reviews and likewise, and so
14 that kind of helps close you know, tactically a gap while
15 the standards are kind of being built into place.

16 MR. PEKOSKE: Okay great, thank you very much for
17 your answers. I appreciate it and Chairman, I yield back.

18 CHAIRMAN CHATTERJEE: Thank you, sir.
19 Commissioner LaFleur?

20 COMMISSIONER LAFLEUR: Thank you. So many
21 questions -- in the interest of time, I'm going to limit
22 myself to one primarily electric and one primarily gas. So,
23 when you talk about increasing the security of the grid, a
24 lot of the talk inevitably goes to retrofitting things,
25 building better fences and adding better control systems and

1 better SCATA and so forth.

2 But right now, a lot of money is being spent on
3 building the grid of the future with all the changes and
4 resource miss and so forth and I'd be interested in comments
5 on how we can actually design the grid to build in more
6 security and robustness and resilience on the front end.

7 I know PJM has been doing a lot of work on you
8 know, the critical substation was one of the standards that
9 was fast -- 72 days. The physical security center had to
10 have a critical substation -- how can we remove substations
11 from that list by building more transmission? I think you
12 alluded to that.

13 But other people are talking about more use of
14 microgrids and certain critical installations like defense
15 facilities and planned islanding in the case of a
16 geomagnetic disturbance, or something broad-based, and other
17 things like that. Can we think, talk a little bit about how
18 we take this back to design?

19 Are there ways we can build the grid better
20 rather than just putting more stuff on top of the one we
21 have? I'll start with anyone, Nick?

22 MR. AKINS: Absolutely, and we should be looking
23 at the grid in a different way. When I grew up in system
24 operations, it was pretty well standard you built generation
25 transmission distribution, you just built more of it.

1 And today though, with the advent of big data
2 analytics, the ability to put monitoring devices on the
3 system -- there's a lot of efficiencies in the system that
4 can be driven out and I actually see that as a resource.
5 And it's one that you can't -- you really have to follow
6 because those advancements are just continuing to progress
7 astronomically.

8 And also, you can't forget the value of the
9 customer themselves and the ability to aggregate different
10 usage patterns and those types of things to enable
11 alleviation of pressures that may occur on the grid. And
12 those are areas that are really in their nesting stages
13 right now that are going to continue to develop.

14 Of course, we're continuing to design in
15 hardening activities, we're putting in transmission centers
16 that are at military spec's and those types of things, that
17 certainly can reinforce the system. But these fundamental
18 changes that are occurring today because of technology, and
19 the technology providers we work with in a very substantial
20 sense -- it's amazing what they come up with.

21 And it's amazing when you see the usage on the
22 grid itself. We can tell you when a facility is going to
23 fail before it fails now. We have asset health analysis
24 that we do and we have real time monitoring that we do that
25 can tell you before it fails and that certainly can

1 alleviate pressure from a system perspective.

2 Those are the kinds of things that continue to
3 develop, and we don't even know all the answers right now to
4 that.

5 MR. GABRIEL: Yeah, I would add Commissioner,
6 thinking differently about the grid is what we're all about
7 these days, right? It used to be you put in a controlled
8 center and we've got four major control centers across our
9 huge footprint, and that control center would sit there for
10 5 or 10 years without much change.

11 Today we are literally tweaking it as we go.
12 It's almost building the airplane as you're flying it. I do
13 believe artificial intelligence is going to be -- is a key
14 already, we've just got so many more inputs, whether it's
15 microgrids, whether it's a military base adding their own
16 generation, trying to keep up with that on a manual basis is
17 going to be virtually impossible.

18 That in using, from our perspective advanced
19 asset management program, getting the data analytics out of
20 the system, so in many cases we're going to operate a little
21 bit closer to the edge, but getting more visibility into the
22 system to understand what that means.

23 So, what does that look like? It means more
24 sensors, more computing power, quite frankly, less men and
25 women physically doing anything because we just can't

1 operate fast enough. That said, I think that at the end of
2 the day we will continue to advance the system, whether it's
3 retrofit, you're retrofitting what we have or in the new
4 spec's -- understanding what that looks like.

5 It's an ongoing process, and one that requires
6 more communications, more intelligence, a deeper
7 understanding of the system characteristics that are out
8 there.

9 MR. GALLOWAY: If I may, there's like three areas
10 that are very consistent with what I think Nick and Mark
11 have said. So, one is kind of improving our planning to
12 kind of reduce risk concentrations, right? So, rather than
13 try to harden you know, those very highly sensitive aspects
14 of the grid, kind of plan those out of the system as best
15 you can.

16 Second is retrofit is very hard, so as we kind of
17 build in new design, especially like large featured things
18 like control centers, we put together you know, work up
19 specific about building out that the next round of control
20 centers, incorporate physical, cyber, EMP-type of hardening
21 at the onset.

22 And then lastly, in terms of equipment design, I
23 think building more interchangeability into equipment going
24 forward, right that kind of works to kind of increase the
25 pool of spares is important. And there's actually been some

1 really good innovative work by several companies -- AEP
2 included, where they'll build modular resilience specific
3 components, not intended for life of the system, but a
4 tactical replacement in the event of a casualty that I think
5 there's a lot of merit in that space.

6 COMMISSIONER LAFLEUR: Thank you, I think that
7 last point is really important because the electric industry
8 collectively has huge buying power and as you get more
9 consistency in the grid in different ways, that helps
10 whatever risk we're facing because you have to -- if you
11 need to rely on your neighbor and so forth.

12 My other question is anyone who has ever managed
13 safety or reliability or anything you're trying to improve
14 knows the importance of kind of learning from near misses,
15 and learning from what happens, and I think that's true on
16 cyber security too.

17 Jim mentioned that we haven't had a loss of load
18 because of the cyberattack, but that's really just the very
19 top of the pyramid because N-kick and others say there's
20 attempts to get in all the time.

21 Recently FERC voted out standards that would
22 require NERC to do -- and the industry, to do more reporting
23 of near misses, and people who attempt to have cyberattacks,
24 as one of the CIP standards. It wasn't super popular as I
25 recall, but I know they're working on it.

1 Is there anything like that in the gas side? Do
2 we know how many people attempt to hack into the pipelines?
3 Is there either mandatory or voluntary reporting to TSA or
4 other agencies that we can even get a handle like, you know,
5 what are the types of things that they're almost happening
6 then we can make it stronger for the next time when a bigger
7 threat vector comes. I know Sonya, who's the best person.

8 MR. SANTA: Currently we request voluntary
9 notification to TSA on attempts to penetrate systems,
10 penetrate the cybersecurity systems. So, there is no
11 mandatory requirement and we have had a number of companies
12 that do voluntarily provide that information to us, we share
13 that information with both the FBI and with CISA, and
14 certainly our intelligence partners often share that
15 information with us. We then try to make sure that we share
16 that information more broadly across the industry because if
17 it's occurring in one place, we want to make sure that we
18 alert the other systems and companies so that they might
19 take mitigating action as well.

20 COMMISSIONER LAFLEUR: Thank you, Don?

21 MR. SANTA: INGA'S members participate in the
22 downstream natural gas ISAC and so that is a vehicle or a
23 forum for information sharing and that information sharing
24 goes two ways. It's not only information sharing from our
25 government partners, but also what are the operators picking

1 up and sharing both with each other but with our government
2 partners.

3 By the same token, I am not aware of any place
4 where a tabulation is kept in terms of the number of
5 attacks, or things of that nature.

6 COMMISSONER LAFLEUR: Well thank you, obviously
7 getting the information is the first step and then kind of
8 figuring out how we learn from it, yes, Nick or Mark, yeah?

9 MR. GABRIEL: Well, you know at WAPA we have a
10 zero-incident culture plan and near miss reporting on the
11 physical safety side. We get 200,000 pings on our firewall
12 every single day. And it's something that we track, both
13 the countries, the locations, the nature. In the last year
14 we identified 10,000 what I would consider to be serious
15 threats, because you can't tell whether it's just you know,
16 sending you some Nigerian Prince thing, or if it's somebody
17 from a foreign actor trying to get in, but it's something
18 we share internally, and then we work in turn to share with
19 our customers who are many of the utilities obviously across
20 that footprint.

21 It grows every single day and it has in the 6
22 years I've been on the job. Those numbers are going up on a
23 continuous basis.

24 MR. AKINS: I've heard mentioned a couple of
25 times there hasn't been a cyber event that caused loss of

1 load here in the U.S. There has been, however, a cyber
2 event that impacted a third party associated with billing in
3 an organized market that we operate it and that became a
4 substantial issue in terms of being able to -- from a cash
5 flow perspective and from a billing perspective, so I guess
6 I'm putting in a plug for CIP 13, because clearly there are
7 parts of the market that are allocated out to third parties
8 that we need to pay particular attention to from this
9 perspective as well.

10 And then we learn as we go along with all the
11 things that are occurring on our system, we're seeing you
12 know, a propagation of malware and those kinds of things
13 that continue to advance and when we see it in the system
14 and you compartmentalize it, we learn something new every
15 time we go through that process.

16 And I think it has to be a regular part of the
17 process and we treat our people who are working in our cyber
18 area just like we do nuclear operators -- they make the
19 decision, they don't make the call to someone else and
20 that's clearly important as well.

21 COMMISSIONER LAFLEUR: Thank you.

22 CHAIRMAN CHATTERJEE: Commissioner Glick?

23 COMMISSIONER GLICK: Thank you Mr. Chairman. Mr.
24 Robb, if I could start with you. In your written testimony
25 you said gas industry regulators should be engaged to

1 establish cybersecurity standards that match those of the
2 NERC reliability standards. Can you elaborate a little bit
3 on your concerns about the cyber posture of the natural gas
4 pipeline system?

5 MR. ROBB: Yeah, and I think I've said this in
6 this forum before. I'm not in a position to evaluate the
7 quality of the regime and mechanisms that are in place on
8 the pipelines. The point that I will underscore though and
9 it is implied in that comment is that it has been mentioned
10 several times by Bruce and others, is that the gas system
11 and the electric system are so intertwined right now from a
12 reliability perspective that the gas system has to have at
13 least the equivalent security reliability to serve its needs
14 as the electric system that's built on top of it.

15 Because we no longer have the rich portfolio of
16 alternative fuels to go after. So, whether it's through a
17 mandatory standards regime, some other regime that with CSA
18 is doing today, or just through the work that TSA is doing,
19 I don't really care so much about that.

20 What I do care about is making sure that the gas
21 is there when we need it.

22 COMMISSIONER GLICK: From an electric grid
23 perspective to the above power system in particular, do you
24 think that if Congress hadn't enacted the 2005 Energy Policy
25 Act and so we didn't have a mandatory standards approach, do

1 you think that we'd be as cyber secure or less cyber secure
2 today?

3 MR. ROBB: I think the cybersecurity standards
4 have been very important in the security posture of the
5 industry. Not in of themselves sufficient, but I think they
6 established a very important baseline to the industry.

7 COMMISSIONER GLICK: So, Administrator Proctor, I
8 just want just to start, you do have the -- TSA does have
9 the authority to impose mandatory standards if it had
10 decided so, correctly?

11 MR. PROCTOR: Yes, sir Commissioner, that's
12 correct.

13 COMMISSIONER GLICK: So, and I'm trying to get a
14 better sense. You had mentioned earlier the benefits of
15 having flexibility and you had also mentioned some of the
16 statistics from your reviews in I guess, FY 2008, you said
17 there were strong indicators that the voluntary approach is
18 working.

19 You said, and I didn't quite follow what you
20 said. Some of the factors you were looking at, there was
21 90% adherence, 85% adherence and 80% adherence. Are those
22 good numbers? Should we be seeking 100% adherence, and is
23 TSA doing anything to ensure that you get to 100% adherence,
24 admitting or knowing that this is a voluntary approach, not
25 a mandatory approach?

1 MS. PROCTOR: Well, I think one of the most
2 important things the Administrator mentioned earlier, is
3 really enhancing the pipeline security group that we have
4 now.

5 So, as a result of the realignment of resources
6 that the Administrator has undertaken, we're going to be
7 able to increase the number of personnel that we have
8 focused on pipeline security which means we will have a
9 presence in the pipeline community on a very regular basis.

10 And that will allow us to get out and do more of
11 the follow-ups on the corporate security reviews, on the
12 critical facilities security reviews, to make sure that we
13 are following up on those recommendations that come from the
14 initial reviews that we do with those companies.

15 COMMISSIONER GLICK: And I feel Mr. Santa, the
16 goal is for inner companies to get to 100% adherence, right?

17 MR. SANTA: It certainly is Commissioner Glick.
18 I mean I think that if you look at the commitments that were
19 made by the INGA Board, I think it reflected that to adhere
20 to the TSA guidelines.

21 COMMISSIONER GLICK: So, if I could go back to
22 you Ms. Proctor, I was trying to understand better the
23 process that based on the GAO report described that TSA
24 uses. So, I understand that you take the top 100 pipelines
25 by through put and then you rearrange those 100, and correct

1 me if I'm wrong here, but you rearrange those 100 by
2 essentially you rank the risk of those particular 100, and
3 then of those 100 you do corporate security reviews and I
4 guess critical facility reviews to the extent those 100
5 pipelines have physical security, critical facilities that
6 they list.

7 Putting aside the 100, what do you do with the
8 rest of the pipeline system around the country, including
9 the distribution pipelines?

10 MS. PROCTOR: Well I would say first of all that
11 through put is one of the major considerations, but clearly,
12 it's not the only consideration in terms of being able to
13 rank the risk for pipelines. As mentioned here, one of the
14 criteria is what those pipelines supply.

15 If they supply an electricity-generating power
16 plant, that's another factor, supply to military bases,
17 their presence in high threat urban areas, so there are a
18 number of other factors that add to the through put factor
19 when we start to rank those systems.

20 So, we don't stop at 100, but clearly you know,
21 we're looking at risk and we're looking at the resources
22 that we have to apply to that risk. So, that is where our
23 focus is first, on insuring that we're looking at those 100,
24 and if necessary, going back to them to make sure that if we
25 find areas where we've made recommendations, when we've done

1 a corporate security review or critical facility review,
2 that they are actually acting on those recommendations.

3 So, they do remain our priority but we are not
4 restricted to those 100, and we will continue to move down
5 that list and we'll certainly have more capability to do
6 that as we have these additional personnel in the field that
7 Administrator Pekoske mentioned, so we're going to have the
8 ability to touch a lot more systems with these additional
9 people.

10 COMMISSIONER GLICK: Which I think is great.
11 Just with regard to the current approach, at least the
12 approach before you added these extra resources, do you at
13 all do any corporate security reviews or critical facility
14 reviews for those other pipelines that aren't in the top
15 100?

16 MS. PROCTOR: We have certainly conducted both
17 corporate security reviews and critical facility security
18 reviews on ones who are not in the top 100. And sometimes
19 we may target -- we may be focused on a company to do
20 critical facility reviews, but there may also be companies
21 in the area that are not in the top 100, but they're
22 physically close by.

23 So, we make arrangements to see if we can visit
24 them at the same time and simply make the best use of having
25 our resources in that area where there are pipeline

1 facilities. So, sometimes we end up going deeper into that
2 list, but it's a proximity issue and it allows us to get
3 beyond that top 100.

4 COMMISSIONER CLICK: Am I correct with regard to
5 the critical facility reviews, that you only do that if a
6 pipeline has identified critical facilities as part of their
7 pipeline system, right?

8 MS. PROCTOR: That is the language that's in the
9 pipeline security guidelines, and that's something that we
10 continue to discuss with the pipeline systems, so that's an
11 area that we continue to work with.

12 COMMISSIONER GLICK: And do you -- if, once
13 they've said we don't have any critical facilities, do you
14 review that at all or that's just based on their word?

15 MS. PROCTOR: We do review that, but we also
16 recognize that a critical facility may fall off the list
17 because of mergers and acquisitions and other redundancies
18 that the companies may have that may eliminate the need to
19 consider a specific facility as critical.

20 So, we take all that into consideration and we
21 look at that when we have our discussions with the
22 companies.

23 COMMISSIONER GLICK: One more gas pipeline
24 question, I promise I won't go on pipelines anymore but, Mr.
25 Santa, I'm assuming INGA doesn't support mandatory

1 standards? I'm curious why that's the case though?

2 MR. SANTA: INGA thinks that the current model --
3 collaborative model with the Transportation Security
4 Administration works well and in fact it is improving. We
5 think that as Assistant Administrator Proctor mentioned, it
6 enables us to be more agile and reacting quickly to things
7 than if we were in a mandatory situation.

8 We also think, and this was something that you
9 know, the Administrator talked about the collaboration, not
10 only with the federal partners, but with others in terms of
11 developing the standards.

12 And one of the things that results from that is
13 that the pipeline operators have some ownership of those
14 standards. It's not an adversarial relationship, it's one
15 where we help to develop those, we buy into them and I think
16 that that is very, very positive.

17 We support TSA in obtaining the resources that it
18 needs to be able to fulfill its mandate more effectively and
19 TSA has agreed to the recommendations in the GAO report, and
20 we think that let's focus on improving that program, making
21 it better, getting it to be what it can be rather than on
22 changing the model.

23 COMMISSIONER GLICK: Good answer, so just one
24 question on the electric side. We're going to talk a little
25 bit more I think about incentives this afternoon and the

1 Chairman initiated a -- through the Commission, initiated a
2 proceeding on transmission rate incentives that we're going
3 to be looking at over the near future, but I'm curious what
4 do you all think that we need to impose incentives, or we
5 need to provide incentives to encourage utilities to make
6 the investments necessary to be cybersecure.

7 Or, do you think the standard setting approach
8 that we use is the right way to go or is there a third way
9 that we should be looking at this in terms of making sure
10 that utilities do what they need to do to be cyber secure?
11 And I don't know who wants to start -- Mr. Akins?

12 MR. AKINS: I certainly think that a
13 transmission-related resiliency incentive mechanism,
14 particularly when you're evaluating all the other
15 incentives, when you think about the future of the grid, the
16 future of the needs associated with it, it certainly helps
17 in that regard because certainly it drives that level of
18 investment.

19 But also, it gives some sense of certainty around
20 what we're doing, and we don't know where all this is going
21 to go -- where the burden of resiliency is going to go,
22 particularly in the cyber and physical world.

23 And to have incentive mechanism that focuses on
24 those actions being taken by utilities not only in
25 compliance but above -- particularly above compliance, are

1 particularly important and I certainly would be supportive
2 of that.

3 MR. GABRIEL: Well certainly from a
4 non-jurisdictional perspective for the PMA's there's not a
5 real difference there. Where we're more interested in
6 making sure that both the standards and the practices, what
7 we do in the industry are followed, because that obviously
8 we interlink with many, many transmission systems for many
9 customers, so incentives aren't are ratio. I will say
10 this. Trying to figure out in our current rate model, how
11 do we make these investments in a way that doesn't drive our
12 rates up so high that it really hurts the customers?

13 MR. ROBB: I'm certainly not going to get into
14 the issues around transmission rate recovery and so forth,
15 but I think the one thing that the Commission might takeaway
16 from my perspective that would advance the ball in a number
17 of ways would be to provide some reward or incentive for
18 utilities that are actively participating, voluntarily
19 sharing information and so forth, because that continues to
20 be one of the limitations of our ability.

21 We can only communicate out to industry what we
22 know. We get a lot of help from our government partners,
23 and that's terrific, but the more we can get from industry
24 itself, would also be very valuable.

25 MR. GALLOWAY: I don't think it's a question of

1 either/or. You know, I think it's a question of both. I
2 would agree with Jim that the mandatory standards around
3 cyber have certainly advanced the industry's posture.

4 But kind of looking at a specific case in point
5 like black start that was referenced earlier. There is some
6 disincentive to owning and operating black start from the
7 compliance burden standpoint, so you want to make sure that
8 there aren't unintended consequences and I think incentives
9 could help balance that out.

10 COMMISSIONER GLICK: I appreciate that, thank you
11 Mr. Chairman.

12 CHAIRMAN CHATTERJEE: Commissioner McNamee?

13 COMMISSIONER MCNAMEE: Right, the benefit of
14 going last is that many of the questions have already been
15 asked. And for the benefit of you all, we're almost to
16 lunch, but my question is I think directed mainly at Mr.
17 Evanina, is that correct, being that my name gets butchered
18 often, I try to be respectful of that.

19 But yeah we heard many people on the panel talk
20 and we've talked about how the grid's being digitized,
21 there's more and more two-way communications, but also as
22 we're becoming more sophisticated, there's more and more
23 entrance points. There are things like you know, from the
24 home, whether it's rooftop solar or whether it's a system
25 that let's you communicate through your thermostat, there's

1 so many new ways for us to interact, but it's also becoming
2 more and more digitized in two-way communication.

3 And we've heard a lot about how this new 5G
4 technology is really going to be a game changer in how it
5 can infiltrate many different things, and I wanted to see if
6 you could talk a little bit because we've heard so much
7 about Huawei, 5G and the threat.

8 What do you perceive as some of the threats in
9 terms of the increasingly digitization two-way
10 communications that every aspect of our electric system is
11 getting?

12 MR. EVANINA: Mr. Commissioner, that's a great
13 question and I will yield my time to others to answer that -
14 - no, I'm just kidding. Huawei and 5G are obviously hot
15 topics these days and my number one concern is the lack of
16 fundamental fidelity we have as Americans and what 5G means
17 and how it impacts our entire core infrastructure or ethos,
18 or ability to communicate or ability to provide energy,
19 what that means downstream -- a lot of key words here.

20 And that means for our ability to have a life
21 with 5G and it's very complex and complicated with the
22 respect there's only a few companies -- countries and
23 companies who provide this capability. I think the
24 criticality of understanding how that's going to be and I
25 will throw in GPS on top of that for ability to move

1 communication networks, nodes, in information and energy all
2 at the same time will all be interdependent.

3 And I think 5G will make that possible for good
4 and will also provide some vulnerabilities that we're not
5 prepared for right now. I'd like to segue a little bit to
6 say that as much as that is, I believe to be an unbelievable
7 critical issue we have from the national security on
8 infrastructure, most important more than that is the entire
9 threat.

10 And I think Mr. Gabriel referenced the fact that
11 the human element witting or unwitting, specifically with
12 the respect to human-enabled cyber will defeat all other
13 aspects with 5G. And I think to segue back to the last
14 question on incentives. If there is, we have a lot of cyber
15 incentives and I think an opportunity for the Commission
16 would look at is potentially, as I Chair and host the
17 Insider Threat Task Force for the U.S. Government, the
18 ability to have an incentive for companies who have insider
19 threat programs that are viable, that have minimal
20 requirements to understand who we're hiring and who we're
21 putting in and amongst our coders, our facilities, or our
22 pipelines, our electrical grids. Who works there?

23 I think it's a dark secret we don't pay attention
24 to in the private sector. We have done an amazing modern
25 effort on this aspect in the government subsequent to 2013,

1 that other's have noted, but we are not all that successful
2 yet.

3 So, we spent a lot of money. We're getting
4 there, but my concern is we have to transition that best
5 practices and those worst practices and lessons learned, to
6 the private sector because I think at the end of the day we
7 look at just some public-facing information, the amount of
8 indictments and arrests since 2019 by the Department of
9 Justice and FBI on insiders -- 22.

10 Not of the government, in the private sector and
11 I think as much as cyber is the shiny object right now,
12 those insider companies that we pay no attention to can
13 cause more harm than cyber can.

14 CHAIRMAN CHATTERJEE: Thank you, thank you to all
15 of our panelists, thank you Administrator Pecoske, Secretary
16 Walker, my colleagues for this. This was a very informative
17 panel. And now we're going to break for lunch, and we will
18 reconvene for the second panel at 1:45 thank you.

19 (Lunch 12:40 p.m. - 1:53 p.m.)

20 PANEL II: Incentives and Cost Recovery for Security
21 Investments

22 COMMISSIONER CHATTERJEE: Alright, I want to
23 thank everybody again for a fantastic start to the session
24 this morning and now I'm pleased to introduce our second
25 panel of distinguished guests to tee up another important

1 round of dialogue and so I'll filibuster for a moment or two
2 longer while Mr. Crane gets situated. You just give me the
3 signal when you're ready, you want to take a sip of water?
4 I will yield the floor to you, thank you sir.

5 MR. CRANE: I'm really glad -- happy to be here
6 today to discuss the investments in the utility industry and
7 what we're doing to make and address cyber physical threats
8 on our nation's infrastructure.

9 The resilient electric power system as we all
10 know, is key to ensuring secure and reliable provision of
11 electricity. Exelon supports the resiliency of the U.S.
12 power system through investments in the transmission
13 distribution network and it's best in class nuclear fleet.

14 We serve over 10 million customers with more than
15 11,000 miles of transmission system. We operate over 20,000
16 megawatts of nuclear generating facilities that have an
17 average capacity factor of 94% and we own one of the few LNG
18 alternatives in Gas Star of New England.

19 The question in the agenda for the panel suggests
20 that a new incentive program might be needed to ensure
21 security-related investments. It is our belief that the
22 electric industry doesn't need a new set of incentives to
23 continue investing in critical infrastructure.

24 Yes, the existing incentives do promote
25 investment. We're much more concerned about securing the

1 current design than looking to add on. This includes the
2 ROE adder for the RTO, which recognizes the benefit of the
3 regional transmission operations.

4 It's the best way for us to have a much more
5 secure and robust grid to be able to lean on the neighbors
6 at times as required. But more important than new
7 incentives, is your support to the day-to-day out processing
8 of rate filings in market rule changes for both transmission
9 and the generating assets.

10 For our transmission assets we need a fair
11 opportunity to recover our costs and earn a reasonable
12 return on equity. We need timely consideration of the rate
13 filings and flexibility when we propose new types of
14 solutions to security's concerns.

15 For example, at Con-Ed we're planning a
16 superconductor cable demonstration project to ensure
17 resiliency in downtown Chicago. While operating at a low
18 voltage -- 12 KV, the project will provide transmission
19 function for looping around substations. And the new
20 technology is partly funded by the Department of Homeland
21 Security.

22 We're asking for the support of this project
23 through a request of the transmission rate treatment and an
24 abandonment protection. So, it's changing a little bit the
25 model of voltage being the threshold and looking at new

1 technology as a new potential to ensure.

2 We're also working with our other transmission
3 owners and PJM to enhance the planning process to mitigate
4 the CIP-14 vulnerabilities. The transmission owners have
5 taken necessary physical measures to protect these
6 facilities as they sit now, but we believe a stronger
7 approach is to upgrade our transmission system, so these
8 facilities are no longer categorized as CIP-14, and we're
9 able to enhance the security of the system.

10 In order to do this without disclosing that
11 vulnerabilities exist, we need to change the transmission
12 planning requirements. PJM transmission owners will be
13 proposing these changes and asking for your consideration.

14 For our generation fleet, timely action or market
15 reforms is important. Our nuclear plant's fuel is secure,
16 they provide around the clock emission's free generation in
17 the harshest conditions, but the increased dependency on the
18 electric system on natural gas for fuel can put the entire
19 system at risk.

20 We are very pro-natural gas, but we have to have
21 the balance as we look forward. Addressing the systematic
22 risk into the electric industry is just as critical as
23 addressing the fiber in the physical threats that loom
24 against us. To address these risks, we need price signals
25 in our energy market that accurately reflect the value of

1 the investment. Indeed, the top recommendation from the
2 August 2017 DOE report on grid resilience was improved
3 market price formation consistent with the recommendation
4 FERC should act on a fast-start reforms that have been
5 pending for some time now.

6 And FERC should give timely consideration to
7 reserve reforms being filed soon by PJM. Changes to the PJM
8 reserve market are needed to ensure supply and appropriate
9 incentives to provide the reserves and reasonably
10 compensated for doing that.

11 If we have a failure of the current PJM rules to
12 reflect -- we do have a failure of the current PJM rules to
13 reflect the value provided by these reserves and it's
14 sending a clear message, unintended we believe, that neither
15 PJM or FERC have that in their interest right now in
16 investment by the generators.

17 Pending the resilience proceeding provided yet
18 another venue for support. In the proceeding Exelon asked
19 FERC to direct the RTOs to perform fuel security studies in
20 their region. To ensure the RTOs are evaluating the right
21 vulnerabilities, federal officials should develop a design
22 basis threat for the RTOs to use to study our ability to
23 withstand the cyber and physical threats.

24 We've gone to great detail and design bases for
25 the transmission with an N minus 1 or an N minus 2, but that

1 starts to fall apart when you add more gas onto the system,
2 and we can't ensure that reliability.

3 Triggered by part of the cost of service filing
4 by our Mystic unit, FERC has directed the New England ISO,
5 which we appreciate to address these issues in a series of
6 compliance filings. Other RTOs, however, are just beginning
7 to look at this fuel security but we believe each is taking
8 an individual approach on how they'll address it.

9 We do need to have the consistency for the design
10 basis for these evaluations so we can ensure that the whole
11 grid is firmly taken care of.

12 Finally, in resilience part about adapting change
13 to system conditions, in some changes such as increasing
14 frequency of the weather events, greater susceptibility to
15 flooding, as we're seeing is being driven by a climate
16 change, no matter what's driving the climate change, we are
17 seeing a climate change.

18 Utilities are responding to these challenges with
19 investments to build more resilient electric power systems,
20 but the states are also looking at ways to mitigate affects
21 of what they believe is the driver of climate change.

22 This includes reducing greenhouse gas in the
23 power sector by supporting emission-free generation. We
24 would ask that the Commission be able to come to grips and
25 address the climate imperatives that the states are driving

1 us to comply with to find a way to work with the market
2 rules.

3 This is the timely way to enhance long-term
4 security of our power sector, so I really do appreciate the
5 time and the opportunity to be here, I made it.

6 MR. BROWN: Well again, thank you for holding
7 this Conference on two topics that are near and dear to our
8 hearts and realizing our mission of keeping the lights on,
9 both physical and cyber security.

10 While the physical security of the network is a
11 primary concern for our members, for SPP in our handling of
12 our responsibilities, cyber is the number one threat -- both
13 in terms of probability of attack and the severity of the
14 consequences should that attack be successful.

15 So, and honestly, it is the only risk in our
16 corporate view of risk management that falls into the high
17 category in both of those areas. So, I thought I'd share
18 briefly my thoughts in three specific areas.

19 One, the regulation of our organization. Two,
20 the security posture of our organization and three, the
21 numerous collaborative arenas that we operate in and some of
22 the challenges that those numerous arenas cause for us.

23 Clearly, we need mandatory standards. There's no
24 question in my mind that we're more reliable and secure
25 today given mandatory standards, than we would be but for

1 that particular situation.

2 But there are two areas of concern that I want to
3 raise and ask for your assistance. And the thing is the
4 threat vectors are changing at increasing rate. You all
5 know that, you hear it all the time. But they're increasing
6 in a vast array of dimensions as well.

7 Technology is moving fairly fast to help us
8 defend ourselves against the growing threats and it's also
9 growing in many dimensions, but our standards are growing at
10 a snail's pace and changing at a snail's pace. So, what
11 does that mean?

12 Quite frankly it means two things. We need
13 flexibility because the standards aren't keeping up with it
14 and we need more timely attention to those standards. Some
15 things move through, particularly if the Commission is
16 behind it, others tend to linger and linger and linger.

17 We have for more than two years, worked with the
18 standard's development team to modify standards that are
19 questionable in terms of current architecture that we've had
20 in place for quite some time that enable us to have within a
21 single security parameter, multiple operation centers.

22 There are many people who support the allowance
23 of this particular technology and yet for more than two and
24 a half years, with no end in sight, that particular
25 modification of this standard has continued to linger.

1 In addition, I think we need more flexibility.
2 We have evaluated any number of products that would enable
3 us to do a better job of protection of system data.
4 Unfortunately, our view of the current CIP standards would
5 not allow cloud-based technologies and yet the vast majority
6 of new flagship products from many of our vendors are
7 cloud-based and have proven the significance of security
8 around those technologies.

9 I believe we need to consider flexibility in that
10 area. And last on reliability and since we're talking about
11 incentives, I would really encourage the Commission to from
12 an enforcement perspective, focus penalties on investments
13 and fixing the problems that you find.

14 I don't doubt that penalties in terms of writing
15 a check are appropriate when there's gross negligence, but
16 when there's not the dollars need to be invested back into
17 the infrastructure.

18 And then I'll move on to collaboration as my time
19 is nearing. We participate at the local level. We
20 participate in the state level with our Arkansas Fusion
21 Center with the Kansas Fusion Center. We participate with
22 DOE and with the FBI and Department of Homeland Security and
23 on and on and on.

24 NERC and CRISP specifically with regard to CRISP,
25 I would really like to see that program become more

1 affordable for more entities. For us it was very
2 cost-prohibitive, it limited how quickly we could move to
3 become part of that program. We have become part of that
4 program but obviously we're all in this together and the
5 more entities that are able to afford to participate in that
6 program, the better off all of us will be in the highly
7 interconnected, highly interdependent network.

8 So, thank you very much, I look forward to your
9 questions.

10 MR. EMLER: Thank you Mr. Chairman, Mr.
11 Secretary, Commissioners, my name is Jay Emler, I'm with the
12 Kansas Corporation Commission. I thank you for the
13 opportunity to share some thoughts with you today about cost
14 recovery, especially in Kansas.

15 What we all do or should states play regarding
16 security -- states should be monitoring the cyber and
17 physical activity efforts of jurisdictional utilities by
18 using such tools as neighbor cyber security survey.

19 That review should be at a level sufficient to
20 determine the efforts are compliant with relevant NERC
21 standards as well as best practices. Utilities in Kansas
22 are statutorily required to provide efficient and sufficient
23 service and therefore have a legal requirement to take steps
24 to protect the networks from cyber and physical attacks.

25 Kansas does not have any explicatively mandated

1 cyber or physical security standards by either statute or
2 Commission order, however, the Commission does have the
3 ability to issue a show cause order to any utility that it
4 believes is not taking adequate steps to protect against
5 cyber and physical threats.

6 The most effective incentives for utilities, and
7 the only ones available in Kansas, are the timely recovery
8 of costs and tracking of O&M expenses. In Kansas, gas
9 utilities are permitted by statute to recover capital costs
10 for security expenses through a gas system reliability
11 surcharge.

12 In addition, several investor-owned gas and
13 electric utilities have Commission authorized surcharge
14 mechanisms to recover O&M expenses related to security.
15 These incentives appear to be sufficient for Kansas
16 utilities to invest appropriately in security.

17 Any new capital investments to address mitigation
18 of emerging threats are covered only under the GSRS statute,
19 and getting timely recovery of costs, since only O&M
20 expenses can be recovered under Commission order and
21 authorized surcharges.

22 However, staff will consider a utility's request
23 for an accounting authority order to defer significant costs
24 that are outside the control of the utility. AAO's are
25 generally used for expenses but can be used in some

1 circumstances for capital investments as well.

2 As long as the utility can provide Commission
3 staff with sufficient rationale supporting the prudence of
4 making investments that go beyond compliance with mandatory
5 reliability standards, staff will most likely recommend
6 recovery of the investment.

7 More specifically, staff would most likely not
8 apply a least cost standard to an energy facility designated
9 as high-risk or critical. The primary factors for
10 Commissions to be aware of, obviously are the threats, the
11 vulnerabilities and the utility's duty of protection,
12 prevention, detection and response to cyber and physical
13 threats.

14 Federal and state authorities should not try to
15 prioritize incentives for security investments. How does
16 the Commission staff know what the appropriate investment
17 may be for a particular company? For that matter, how do
18 the Commissioners know? Those are decisions that are best
19 left to the utilities.

20 Timely recovery should provide sufficient
21 incentives for utilities to meet the legal obligation for
22 efficient and sufficient service. What states and the
23 federal government can do, is facilitate public, private
24 partnerships such as the Kansas Intelligence Fusion Center.

25 Information about the most serious threats to

1 critical infrastructure will never be unclassified. The
2 private sector needs more staff clearances to fully
3 understand the nature of the threats and to objectively
4 compare those threats to the company's defenses.

5 The underlying question that any company should
6 ask is how does this threat affect my company? No company
7 should expend funds for defenses unless it can answer that
8 question, and no Commission should approve recovery of
9 expenses unless the company can explain the necessity.

10 CRISP is a good, tactical tool for today. The
11 classified environment provides strategic tools to plan for
12 tomorrow. This marriage of utility operations and
13 intelligence knowledge is a fledgling science, but it has
14 proven so effective the Kansas Corporation Commission is
15 funding an analyst position in the Kansas Intelligence
16 Fusion Center to assist Kansas utilities.

17 We strongly believe protection of critical
18 infrastructure is protection of our nation, thank you.

19 MR. WAILES: Thank you Mr. Chairman. My name is
20 Kevin Wailes. I'm the Chief Executive Officer of the
21 Lincoln Electric System in Lincoln, Nebraska and I'm also
22 privileged to serve as the Co-Chair of the Electricity
23 Subsector Coordinating Council, which you've heard reference
24 to several times today.

25 LES is a greatly integrated electric municipal

1 electric utility serving about 140,000 customers in Lincoln
2 and the surrounding communities and are a transmission owner
3 member of SPP, so we're kind of the other end of where CRISP
4 is.

5 With limited exceptions, public power utilities
6 like LES are not subject to state public service commission
7 rate jurisdiction. Public power utilities are also
8 generally excluded from the Commission's rate jurisdiction
9 under the Federal Power Act, although some public power
10 utilities, including LES, recover transmission revenues
11 through RTO or ISO rates.

12 Rates for public power utilities are generally
13 set by citizen-controlled boards or city councils. As we
14 talk about cost recovery in incentives, it's important to
15 keep in mind that public power utilities may be paying these
16 costs through their transmission and other wholesale rates,
17 and those costs are going to be on top of the infrastructure
18 costs incurred by public power utilities for their own
19 systems.

20 Public power utilities as a group, maintain a
21 healthy financial profile and ability and demonstrate a
22 willingness to adjust rates to recover necessary expenses as
23 has been recognized as a strength of the public power
24 business model.

25 At the same time, we must remain mindful there

1 are limits to costs that we can reasonable ask members of
2 our communities to bear. In considering investments to
3 promote physical and cybersecurity, public power utilities
4 like other utilities, must weigh the security risk to
5 utility infrastructure against the potential cost
6 constraints on investments that might mitigate those risks
7 and the adverse effects should an incident occur.

8 A key component in striking that proper balance
9 is having dependable information and awareness considering
10 the threats the industry faces, and informed approaches to
11 mitigate those threats.

12 As an ESCC Co-Chair, I know that you all are
13 familiar with the roles ESCC plays in facilitating
14 information sharing, cross sector coordination, planning for
15 resilience response and recovery and working with our
16 government partners. Facilitating access to reliable threat
17 awareness information to the SCC and other programs can
18 inform the appropriate investment and adoption of best
19 practices for cyber physical security by public power
20 utilities.

21 In my experience, public power utilities are
22 willing to make necessary and risk appropriate investments
23 to promote infrastructure security in a local rate setting
24 process used by most public power utilities allows them
25 thwart those investments.

1 I believe there is a role for state and federal
2 governments to play in supporting utility investment and
3 infrastructure security in certain cases. In my experience,
4 relatively small investments by the government can pay big
5 dividends in promoting infrastructure security even where
6 the dollars are not spent on specific facilities.

7 As an example, in 2016, the American Public Power
8 Association entered into a three-year cooperative agreement
9 with DOE that provides APPA with funding to help public
10 power utilities create stronger, more cyber secure cyber
11 systems. The program is particularly valuable for small
12 public power utilities, many of which there's concerns
13 identified as you well know in the industry.

14 I cite the DOE/APPA agreement as an instance
15 where, in my view, targeted support for industry initiatives
16 has really moved the needle in promoting infrastructure
17 security. The case for making incentives to encourage and
18 prioritize infrastructure investments I think is less
19 compelling. In fact, I would be concerned that rate
20 incentives could influence utilities to focus on the wrong
21 things, possibly not making the investments correct with
22 respect of where the risks are because of driving those
23 incentives -- driving them there.

24 I think we can all agree that public utilities
25 should not receive any incentives for security investments

1 to meet the existing standards. However, I think we also
2 know that the majority of the industry is going far beyond
3 the standards in working toward and aggressively working to
4 exceed standards and make the system safe.

5 I think that if we consider funding specifically
6 for different types of initiatives, and maybe like the
7 program mentioned with DOE, maybe for enhanced information
8 sharing, it may very well be for DCEI facilities where you
9 really don't want to socialize those costs across the
10 utility, you need to have target specific funding for those,
11 or specific funding for other kinds of retrofit
12 infrastructure investment that's already targeted.

13 Another thought that I had that is I guess
14 similar off of this, and I know we're all concerned about
15 the amount of engagement by the industry. I think if you
16 look at all the people here and you take LAS as an example,
17 where 140,000 customer utility -- we, if you look at our
18 relationships, I've served on ESPC with Chris and Nick for
19 several years.

20 We're a customer of SPP. We actually are engaged
21 in the Kansas Fusion Center, although we're in Nebraska.
22 They actually don't limit the participation in working with
23 them as well. We're a customer of Mark, the Western Area
24 Power Administration when he was up here. We're obviously
25 regulated by NERC. I also have a relationship with the

1 ISAC.

2 So, and actually to think of it we were -- Chuck
3 Kosak, with respect to his integration with the ESCC as
4 well. So, when you look at the combination of a utility our
5 size and working across that, I think you've got a good
6 example of how seriously the industry takes this.

7 We're not waiting for incentives to make our
8 moves, we're trying to do those now to make things better.
9 Thank you for your time.

10 MR. KJELLANDER: And good afternoon, my name is
11 Paul Kjellander, I'm a Commissioner with the Idaho Public
12 Utilities Commission, and thanks for letting me be here
13 today.

14 As I see the shock clock, I'm reminded that today
15 is the first day of opening day of major league baseball and
16 in spring training this year they actually experimented with
17 a shock clock to try to speed up the game. And when the
18 media interviewed one of the managers, he said they're
19 over-thinking it. All they really need to do is make it a
20 7-inning game.

21 And I think that's relevant to my main point
22 today. And my main point is that as state regulators, we
23 don't have to invent new rate recovery tools to recover
24 cybersecurity costs, we just need to be willing to utilize
25 the ones that we have as the situation warrants.

1 And so, what I'd like to do is just touch on a
2 couple of the rate treatments and rate recovery mechanisms
3 that we utilize and how they might be relevant. I'll touch
4 on base rates, annual cost adjustments and single-issue rate
5 cases, and also touch on regulatory pre-approval processes
6 that we have in our state in Idaho.

7 Let me start first with base rates. That seems
8 to be the most common around the states as built-in recovery
9 costs in the base rates, and there are some concerns though
10 as we look at a base rate environment that might represent a
11 disincentive for some investment.

12 One of the obvious concerns is that in the
13 evolving world of cyber threats, the amount of rate base
14 might not be enough to cover costs and expenses. The
15 cybersecurity costs are one of the only items that are
16 potentially out of line -- the cost to put on a full-blown
17 rate case to recover extraordinary costs might serve as a
18 huge deterrent to appropriate investment.

19 Another perceived risk of opening up a full-blown
20 rate case to address cybersecurity costs is the risk that in
21 an effort to keep overall rates low, the amount of recovery
22 that regulators allow in other areas of the utilities
23 operations could be lowered to find the money for increased
24 cyber costs.

25 This type of trade-off could create problems

1 elsewhere for the utility, and the outcome for the utility
2 might be one they don't want to risk. The final perceived
3 concern with a rate base approach, is the potential
4 disincentive that depreciation schedules might have on
5 investment, especially if there's a huge gap in time
6 between rate cases.

7 One way to address this concern is to establish
8 deferral and tracker accounts and this type of accounting
9 treatment is very easily set up and it helps reduce the
10 perceived risk that appropriate costs won't be recovered.

11 I'd like to touch next on annual cost adjustments
12 or potential riders with true ups. An annual adjustment --
13 cost adjustment really isn't a new concept for state
14 regulators. We've used it for years now with fuel cost
15 adjustments.

16 But the reason we use them is when we have some
17 widely varying costs year-to-year. And so far, we haven't
18 necessarily seen that occur with cybersecurity costs. That
19 doesn't mean we won't, and certainly we do I think as state
20 regulators, want to keep an eye on what we're seeing in the
21 industry as cybersecurity costs migrate from capital
22 purchases to O&M expenses, the software companies move to
23 subscription model and cloud-based resources.

24 To the extent then that that creates more of a
25 potential wild swing year to year, perhaps maybe an annual

1 cost adjustment is worth considering. One of the areas that
2 I think has some merit are the one-off rate cases for a
3 single issue. We see those occasionally. I know a lot of
4 state regulators don't like them. I'm becoming more-fond of
5 them though if we can actually use them to ensure that the
6 appropriate incentive is being made for something as
7 important as cybersecurity.

8 With the single-issue rate case too, as far as
9 managing that case from a regulator's perspective, every
10 party that is in the room has the clearance to be there, so
11 you're not constantly having to clear the hearing room when
12 a witness that might have multiple areas in a major rate
13 case that he's covering and you start to get into
14 cybersecurity issues.

15 So, from a management perspective it could be
16 more efficient as well. The last area that I do want to
17 touch on too is just with the regulatory pre-approval
18 process. I think that gives the investment community a lot
19 of certainty that those costs will be recovered, and I think
20 that's important for everyone across the board because
21 obviously we don't want to see costs of capital go up as a
22 result of some concerns about non-recovery of costs.

23 I was told to try and say something provocative,
24 so here goes. When -- something to consider is that when
25 FERC, NERC or WEC issue a substantial penalty for critical

1 infrastructure protection violations, I'm wondering if there
2 couldn't be an emphasis on allowing those utilities to
3 perhaps come up with a negotiated settlement so that instead
4 of using that fine as a punitive measure, instead use that
5 as investment into the capital improvements that might be
6 necessary to resolve the problem. I think that would go a
7 long way to ensuring that there is an incentive there, and
8 again move away from the punitive nature of a potential
9 fine.

10 What you also see in that environment too is when
11 a fine is issued, a state regulator looks at that and says
12 that goes straight to shareholders, so that immediately
13 impacts the ROE, the return on equity and ultimately the
14 revenue and it's unrecoverable.

15 So, if there was actually an investment set up in
16 that incentive, there might be a possibility for them to
17 seek recovery through some of the other recovery mechanisms
18 that states have and it wouldn't just be a lost cost. So,
19 something to consider.

20 The last thing I'd like to bring up now that I'm
21 over time is that as state regulators, we used to have a lot
22 of authority as it related to telecommunications, and I know
23 that earlier today there was a conversation about the
24 telecommunication sector needs to be heavily engaged in this
25 if we're to be successful.

1 The problem we face at the state level is that
2 that regulatory authority is largely removed from state
3 regulators and our ability to actually mandate them to show
4 us what they're doing doesn't exist. That doesn't mean that
5 they won't provide us some assurances and that doesn't mean
6 we have bad players, it simply means that states don't have
7 that regulatory authority like they once did in order to
8 assure citizens and everyone else that they're playing and
9 participating in the manner in which we think they need to
10 going forward to help avoid cybersecurity risks.

11 So, those are my comments. I really apologize
12 for going over, but Commissioner Chivukula said he'd shorten
13 his to accommodate me.

14 CHAIRMAN CHATTERJEE: I would point out that
15 moving to 7-inning games is the most provocative thing that
16 you said.

17 MR. ARMSTRONG: Good afternoon, my name is Alan
18 Armstrong. I'm the President and CEO of Williams. Thank
19 you, to discuss a sensitive and important topic of physical
20 and cybersecurity of the nation's natural gas pipeline
21 systems.

22 Industry and government both have a role in
23 ensuring pipelines make the necessary investments to keep
24 our system secure. The investments we've made to date have
25 served our systems very well. In fact, Williams has in

1 place a strong program that relies on effective protocols
2 and redundant, but isolated systems to protect the service
3 to our customers.

4 Williams today owns and operates premiere energy
5 infrastructure across the United States, including the
6 Transco and Northwest Pipelines, two interstate natural gas
7 pipelines regulated by this Commission, with Transco being
8 the largest volume and fastest-growing interstate pipeline
9 system in the U.S. Williams has over 33,000 miles of
10 pipelines and we are sharply focused on continuing to build
11 out and operate large scale natural gas infrastructure and
12 in fact today through both our regulated and our
13 unregulated systems here in the U.S. today, we handle about
14 30% of the nation's natural gas.

15 Cyber and physical security is a high priority
16 for Williams. We recognize that our industry, like many
17 others, faces a constantly changing threat landscape, and
18 increasingly sophisticated and adaptive adversaries.

19 Williams acknowledges that these threats not only
20 present a risk to Williams, but also have the potential to
21 impact national security, the environment and public safety.

22 To address these threats, Williams applies a risk-based
23 approach to protect our facilities and the technologies that
24 support our operations.

25 Williams cyber and physical security programs are

1 oriented around the TSA pipeline security guidelines and the
2 NIST cybersecurity framework and include effective
3 governance, comprehensive risk-based management and numerous
4 programs designed to promote the security, reliability and
5 resiliency of our operations.

6 Williams has physical redundancy in both our soft
7 and our hard control systems, and incorporates numerous
8 layers of defenses, back-ups, fail safes, and manual
9 controls to ensure that we can safely keep gas flowing even
10 if associated computer systems such as our SCADA systems,
11 become unavailable.

12 We maintain back-up control rooms, and back-up
13 data rooms in geographically dispersed locations, in fact
14 thousands of miles apart to enable quick recovery in the
15 event of a successful cyber intrusion and conduct regular
16 incident response exercises to improve our readiness and
17 insure the resiliency of our operations.

18 The fact is that natural gas transportation
19 systems are designed to limit points of failure and ensure a
20 very high degree of reliability and so just as you heard
21 from Nick Akins with AEP this morning, we very much see our
22 brand as a brand reliability.

23 We serve very important markets, we understand
24 that and we take our brand of reliability very serious with
25 or without regulatory insistence on that.

1 So, let me provide a real-life example of what
2 actually goes on around our systems. We recently
3 experienced an extended outage in our Transco Houston
4 office, and this is our control room where we actually
5 managed the Transco system and we had a building
6 maintenance item that actually caused the fire suppression
7 system in our control room to be activated.

8 And we actually had a very extended outage on our
9 system. You didn't hear about that because we both
10 immediately transferred control to our local operations,
11 maintained control of our system and then we very quickly
12 moved that control center to one of our redundant control
13 systems that was thousands of miles away from that location.

14 So, we are very prepared, and we take very
15 serious --our ability to monitor that. And I raise this
16 issue of both the redundancy and our ability to recover from
17 that because a lot of the concern that exist is very
18 important, we take it very serious, we hear very often from
19 the intelligence community around threats and major concerns
20 that we should be aware of, and -- thank you, and so, we are
21 constantly on the edge for those issues.

22 However, I would say probably the most important
23 thing that we should note, convergence of knowledge between
24 the intelligence community and the knowledge that we have as
25 operators about really where our vulnerabilities are, really

1 needs to be brought together.

2 And if there's anything that we can do through
3 this effort, I would tell you that the convergence of that
4 knowledge, and more open sharing about where those concerns
5 exist, is what Williams would point you to.

6 Relative to the cost recovery issue, I would tell
7 you that we think that the 2001 policy statement on
8 extraordinary expenditure is necessary to safeguard national
9 energy supplies, does support our pipelines adequately, and
10 we do not feel like there's anything broken today in terms
11 of our ability to recover cost.

12 I would raise, however, though there are many
13 areas where there's very stiff competition such that we can
14 raise our rates and get that cost recovery, but we can't
15 necessarily push that through to our customers and so I
16 would just raise that as a concern as well.

17 And with that I thank you very much for the
18 opportunity to speak to you today.

19 MR. CHIVUKULA: Good afternoon, my name is
20 Upendra Chivukula. I'm a Commissioner on the New Jersey
21 Board of Public Utilities. I would like to thank the
22 Chairman, and Commissioners and members representing
23 yourself, Department of Energy and the FERC. I would like
24 to thank Joe McClelland and the FERC for providing me this
25 opportunity to share my thoughts in this panel as we explore

1 how federal and state authorities can provide incentives and
2 cost recovery for security investments in the energy
3 infrastructure.

4 I'm very proud to state that New Jersey Board of
5 Public Utilities was the first state to issue a
6 cybersecurity order in March of 2016, specifying
7 cybersecurity program requirements, cyber risk management,
8 maintaining situational analysis, incident reporting,
9 response recovery and security awareness training.

10 A significant amount of utility infrastructure at
11 risk falls within the purview of the state public utility
12 commissions who work to ensure safe, reliable, adequate,
13 utility service at reasonable rates.

14 PUC's must make sure utilities are investing in
15 security and insure those state investments are prudent.
16 Security mitigation can be accomplished by using a variety
17 of mitigation techniques, including administrative controls
18 such as policies as well as technologies.

19 For example, automated threat monitoring systems.
20 To execute their cybersecurity related responsibilities,
21 PUC's must first know utilities business risk profiles which
22 include current and emerging physical or cybersecurity
23 threats and vulnerabilities and also have a working
24 knowledge of best practice mitigation techniques.

25 Information sharing specifically about threats

1 and actual and potential incidents is crucial for PUC's to
2 be successful in this regard. With federal partners,
3 including Department of Homeland Security, Department of
4 Energy and FERC, which specific sector information sharing
5 and analysis centers, ISACS and with the utilities
6 themselves.

7 Armed with the cybersecurity knowledge, PUC's can
8 assess utilities physical and cybersecurity preparedness and
9 make prudency decisions. Physical attacks could render
10 parts of the grid out of service for some period of time.

11 Examples of physical attack on Metcalf Substation
12 California, the unrealized, low-probability, high
13 consequence threat of electromagnetic pulse attack.
14 Cyberattacks, America's intelligence community is raising
15 alarms about cyber threats to critical infrastructure.

16 The worldwide threat assessment by Daniel R.
17 Coats, the Director of National Intelligence, contends that
18 China is able to launch cyberattacks that cause localized
19 temporary disruptive effects on critical U.S. infrastructure
20 such as destruction of a natural gas pipeline for days to
21 weeks, and that Russia is able to execute cyberattacks on
22 electrical distribution networks similar to those
23 demonstrated in Ukraine in 2015 and 2016 and is mapping out
24 a critical infrastructure with long-term goal of being able
25 to cause substantial damage.

1 And going forward I think one of the things I
2 want to say is that PUC's also must evaluate security
3 preparedness in terms of risk of reliability and safety and
4 cost to customers and so also PUC's need to conduct many
5 black sky exercises to examine response and recovery roles
6 and responsibilities and information sharing that way.

7 And resilience is an important thing. PUC's need
8 to actually be discussing cybersecurity resilience, what it
9 is, how to measure it and how to incentivize it in examining
10 the various risks associated with infrastructure
11 interdependencies.

12 Cost recovery also means incentivized security
13 preparedness as my colleague Commissioner Scott Emler said -
14 - I'm also losing my time, the range of cost recorded
15 mechanisms for security investments is well known. The most
16 familiar one is filing a general rate case and that is the
17 best we know so far.

18 In 2017, national renewable energy laboratories
19 suggest that among those surveyed the base rate is the most
20 popular mechanism for recovering cybersecurity expenses. It
21 was selected by 10 out of 22 utilities and 8 of the 19
22 non-utilities. PUC's are working with National Association
23 of Utility Commissions, that is working to advance PUC's
24 knowledge of physical and cybersecurity risks and has
25 awareness of best practice risk management practices and

1 provides tools to assess utilities implementation of those
2 practices.

3 And also, is offering cybersecurity training for
4 regulators so that way the regulators can obtain working
5 knowledge needed for utility oversight and in 2018 NERC's
6 survey with 21 PUC's responding, found that half of those
7 responding have legislation rules, administrative orders
8 requiring utilities to provide information on cyber
9 practices, threats and incidents to the PUC.

10 It also required auditing, evaluations and
11 assessments of utilities, cyber security capabilities. And
12 of course, the capability most often assessed against NERC's
13 CIP and in this cybersecurity framework.

14 Bottom line here is that the -- when you're
15 investing in cybersecurity, especially in terms of federal
16 government incentivizing, it impacts the rate payer in the
17 states like New Jersey we are already paying very high rates
18 and whether you are giving already adders and things like
19 mechanisms like that, it really comes down to the bottom
20 line of the ratepayers.

21 And so, you need to be cognizant of that and so
22 that way we don't get unduly burdened and punished because
23 of some of the policies at the federal level. Thank you,
24 Chairman.

25 CHAIRMAN CHATTERJEE: Thank you all very much for

1 another excellent panel. I'll jump right into the Q&A.
2 From time to time I hear concerns that utilities may not be
3 able to recover their costs for cyber and physical security
4 expenditures. Since the events of September 11th, I think
5 this Commission has been very accommodating in providing a
6 number of mechanisms for utilities to recover the costs of
7 their prudently incurred security expenditures.

8 That includes things like formula rates and
9 single-issue rate-making just to name a few. So, my
10 question for the panel is this. Are there really barriers
11 to recovering the costs of security expenditures, or are the
12 concerns on that issue overblown?

13 MR. CRANE: We have not, at Exelon, our 6
14 utilities have not experienced any issues with recovery on
15 the prudent investments around the physical and
16 cybersecurity. A lot of our focus in early on investments
17 have been on the transmission side where the formula rate
18 has worked very well for us as we address the CIP-14 on the
19 distribution side as we encrypt more of our -- all of our
20 components, our automation components, we've been able to
21 recover those.

22 So, we haven't seen a problem in the states that
23 we operate in.

24 MR. EMLER: I don't believe in Kansas, as I
25 mentioned that there is a difficulty. We either allow it

1 through what would be a rate case or through a rider. The
2 issue may be really just one of timing, but in terms of
3 actually recouping the costs, I don't think that it's been
4 an issue, it certainly hasn't been mentioned to me that it's
5 an issue other than timing of the recovery.

6 MR. CHIVUKULA: Chairman, that's not the case in
7 the State of New Jersey. We have all the utilities quite
8 engaged in our -- the cyber security order in 2016 and not
9 once we hear from them saying that we have all the
10 requirements and mechanisms, it would incentivize them.

11 MR. KELLANDER: And Mr. Chairman, you know as a
12 state regulator, at least I don't, and I don't think many of
13 my colleagues do. We don't try to micromanage the company,
14 so it really is up to the utility to let us know if they
15 think that there's a problem with cost recovery.

16 We haven't heard anything on that front, however
17 if a company were to be out from a rate case for 4, or 5 or
18 6 years, and hadn't set up some kind of deferral or tracker
19 account, there's a possibility that some of those costs
20 might not be recoverable and those are things I think we
21 need to look at going forward.

22 But as of today, we're not hearing any major
23 problems as far as the ability for them to come and seek
24 recovery.

25 CHAIRMAN CHATTERJEE: Thank you. Unlike FERC

1 transmission rates which tend to use formula rates, I know
2 that gas rates tend to be at negotiated rates, or stated
3 rates set by a rate case or settlement. So, Mr. Armstrong,
4 given those differences, are there more difficulties
5 recovering the costs of security investments for gas
6 pipelines?

7 And if so, is there anything FERC should be doing
8 differently?

9 MR. ARMSTRONG: Great question and thank you for
10 that. You know I think the trackers that have been put in
11 place for incidents, for instance within Williams, we had a
12 tracker for some hurricane damage that was very effective.

13 A different situation but very effective in being
14 able to push that through and a non-discounted way. It is
15 true though that it is, there are definitely spots within
16 the industry that are very competitive and you can raise the
17 rate all you want to and there's inability to push that
18 through.

19 So, I wouldn't dodge that, you know, implication.
20 I would say we're not aware of any situation today within
21 Williams or within the INGA member companies where people
22 are not making adequate investment in keeping the systems
23 reliable and safe because they realize how incredibly
24 important that is.

25 I will go back to my previous comment however,

1 about not knowing exactly what risks might be in part we
2 hear the comment from General Coats, some of these comments
3 about there being things that we're unaware of, it's very
4 hard for us to predict what the cost of that would be if
5 we're not aware of exactly what those intelligent concerns
6 are.

7 I would say of the things we are aware of, we
8 feel like we've got the ability to recover those in cost and
9 within some of the structure and again the 2001 policy for
10 extraordinary expenses that the Commission wisely put in
11 place.

12 So, it is a real issue, but I would say at the
13 levels that we're investing today, it's not problematic.

14 CHAIRMAN CHATTERJEE: You mentioned earlier in
15 your testimony that the source of frustration -- the
16 knowledge gap that sort of occurs that you hear gloom and
17 doom about potential vulnerabilities in these intelligence
18 briefings, but you don't necessarily have access to the
19 highest levels of intelligence, so it's hard to know if
20 you're investing in the right areas to assess those
21 vulnerabilities?

22 MR. ARMSTRONG: Correct, and I would just say
23 there's a lot of room in between the very specific
24 instances, IP addresses that are sensitive and things like
25 that. We're not really, from a Williams perspective, or an

1 industry perspective, we're not all that concerned about the
2 who in the attack. We're concerned about the mitigation of
3 the attack, and so I would just say the very nature of the
4 concerns could be shared with us in a way that I'm not sure
5 would be all that sensitive, because we obviously see
6 attacks against our system every day and so we've got our
7 eyes on that.

8 We're constantly repelling those attacks and
9 we're aware of that. If there's something else that we're
10 not aware of and don't even have our defenses up, it really
11 would be nice to know what those are, so yeah -- and
12 likewise, I think it would be nice for the intelligence
13 community to really understand how our systems operate so
14 that they really would know where those Achilles heels
15 really are and really aren't.

16 Sometimes, some of the concerns that when we have
17 gotten close to them, really haven't been things that could
18 take down our whole systems in a way that might have been
19 feared to be the case.

20 CHAIRMAN CHATTERJEE: Maybe that's something
21 Assistant Secretary Walker and I can follow-up on. Circling
22 back, Commissioner Emler, you mentioned in your testimony
23 that Kansas allows gas utilities to recover capital costs
24 for security through a surcharge. How does that work in
25 your state and have there been any lessons learned that

1 would be helpful to others that may be considering a similar
2 mechanism?

3 MR. EMLER: It's called the Gas System
4 Reliability Surcharge, the GSRS. It's been in place for
5 about 9 years I believe. It is limited, there was concern
6 at the legislative level that gas companies might put more
7 into the surcharge than would be appropriate.

8 So, it was limited to 40 cents per month, per
9 customer. This year or this past legislative session that
10 was up to I believe now 80 cents -- which isn't really high
11 enough probably to get as much done as quickly as it
12 probably ought to be, but I would say that it's probably
13 working, just more slowly than the gas companies and
14 probably the customers would like to see.

15 CHAIRMAN CHATTERJEE: It's very helpful. Mr.
16 Crane, in your remarks you mentioned the importance of using
17 the transmission planning process to eliminate or reduce the
18 criticality of certain substations or other elements. I'm
19 very exciting, you know, about the possibilities for new
20 transmission in this country on the potential economic and
21 resilience benefits it can provide.

22 But obviously, building transmission can also be
23 very expensive, so how do we identify that sweet spot where
24 we reduce the criticality of individual facilities but we're
25 not gold-plating the system?

1 MR. CRANE: Yeah, it's not our intent in our
2 transmission planning process that we utilize to gold-plate,
3 but to ensure we're doing everything to remove the
4 vulnerabilities. We serve, as you know, some pretty
5 critical assets, cities, and being able to assess those
6 CIP-14 assets and look at cost effective alternatives has
7 been our focus.

8 The advancing technology using more capabilities
9 of that advancing technology like super conductors, things
10 like that, are economic fixes that can drive reliability and
11 ensure the safety of the system as we go forward.

12 It's through the planning process and through
13 what we use at the RTOs, there is that balance of what's the
14 best methodology to perform this when we're dealing with
15 this CIP-14 issues as I discussed earlier.

16 There is an issue on the transmission planning
17 about the openness of how we have to identify the
18 vulnerabilities and attack those, but we do have a process
19 where we justify the work that's being done and show that
20 other alternatives going forward, we just need to be allowed
21 to do that in a more confidential way.

22 CHAIRMAN CHATTERJEE: Very helpful, thank you. A
23 number of you have mentioned the benefits of the CRISP
24 Program, and also, it's relatively high cost. Mr. Brown, in
25 his testimony suggested the idea that FERC encourage

1 mechanisms to subsidize or otherwise make that program more
2 affordable for utilities.

3 So, I was curious whether the panel had any
4 suggestions on how FERC or DOE might be able to do that,
5 happy to start with Mr. Brown since it was your idea, and
6 then open it up to others.

7 MR. BROWN: Well I wish I had all the answers to
8 that. All I can do is point to the number of years that
9 we've wanted to participate, but it was cost prohibitive.
10 Finally, there were enough larger utilities that
11 participated that our initial cost was down to \$300,000 a
12 year and ongoing, \$180,000 a year.

13 But again, we're all in this together and the
14 more people, the more utilities that are able to
15 participate, the better off we're all going to be. I'm not
16 sure if that comes through just reducing the rate, an
17 attempt of almost build it and then they will come or what.

18 But I personally believe something needs to be
19 done to accelerate the participation in that program.

20 CHAIRMAN CHATTERJEE: But you affirm the value is
21 there?

22 MR. BROWN: The value is absolutely there. Our
23 folks are dead set on that.

24 CHAIRMAN CHATTERJEE: Any others with
25 suggestions?

1 MR. EMLER: Obviously, Bruce would be better
2 placed, probably to answer similar questions with respect to
3 this, but it seems to me that there also is the opportunity
4 for additional DOE funding itself with respect to that since
5 it's actually a nationwide program that's supporting
6 bringing all that information and data into one point and
7 then distribute it back out to the users.

8 So, that is a possibility as well as if there's
9 additional funding to be applied from the government side.

10 CHAIRMAN CHATTERJEE: Maybe a coupon Secretary
11 Walker?

12 MR. WALKER: Sure, you're going to get in the 8th
13 inning.

14 CHAIRMAN CHATTERJEE: The states obviously have a
15 critical role in cybersecurity because of their authority
16 over the distribution system and then also their role in
17 setting retail rates. So, to the Commissioners, could you
18 talk about how your states have been considering investments
19 for physical and cybersecurity and particularly, how you
20 evaluate requests for cost recovery?

21 MR. KJEELLANDER: I'll ramble on first. There
22 really hasn't been anything out of the norm over the last
23 few years. Again, I don't know what we'll see going
24 forward. What we're hearing from the utilities is that
25 because there is a shift now in a lot of the software

1 providers to do subscription-based and to move into a
2 cloud-based services, that there's some concern about how
3 those will be treated going forward, and some conversation
4 about whether or not there should be a different type of
5 regulatory treatment to allow those to be recovered with a
6 return on investments, similarly as you would the capital
7 expenses.

8 That hasn't actually shown up to us yet, but
9 we're not really hearing anything out of the ordinary yet.
10 A lot of the concerns we're hearing though about the
11 distribution system as we're trying to wrestle with this,
12 we're still trying to deal -- and I think it was
13 Commissioner LaFleur who brought this up with some of the
14 other issues about integrating anymore distributive
15 resources into the system and how that's actually driving a
16 lot of the investment now.

17 So, the question comes as is certain investment
18 going to happen because of immediate concerns and needs they
19 have versus investment here and that's something we just
20 want to be watchful of going forward.

21 CHAIRMAN CHATTERJEE: Kansas and New Jersey?

22 MR. CHIVUKULA: In New Jersey we have several
23 focus group meetings of the utilities when we are preparing
24 the cybersecurity order. The question of cost recovery
25 often came up. We allowed a multi-phase in requirements

1 that provided two budget cycles for utilities if they needed
2 to acquire additional resources to meet all the
3 requirements.

4 We also signaled the utilities that we would
5 consider alternate recovery mechanisms should a case warrant
6 and so far, we haven't had the opportunity.

7 CHAIRMAN CHATTERJEE: Mr. Emler?

8 MR. EMLER: I would concur that we haven't seen
9 anything earthshattering from any of the utilities but given
10 an example, one of the utility use asked to meet with me and
11 told me that they were looking at a vendor that wanted to
12 charge them 3 million dollars for a particular product and
13 after they reviewed the product, they told me that the
14 \$500,000 that they'd spent over a few years with the Fusion
15 Center was far more effective.

16 Now, whether they were just blowing smoke because
17 of my connection to the Fusion Center, I don't know. But I
18 believe that they were quite serious that they were being
19 very cost conscious, and they didn't purpose the 3
20 million-dollar product, but they did continue the
21 relationship with the Fusion Center.

22 So, our staff takes a look at was the expense
23 reasonable? Was it out of the ordinary? And could the
24 company justify why they spent the dollars they spent? I
25 don't think that we've seen a problem from any of our

1 jurisdictional utilities as far as recovering the cost.

2 CHAIRMAN CHATTERJEE: Having been to the Fusion
3 Center as a guest of yours and Representative Tom Sloan's I
4 can honestly say I agree with their assessment that you do
5 tremendous work there, there is tremendous, tremendous
6 value.

7 My final question -- in some instances the states
8 have looked to FERC for guidance on how to approach certain
9 issues. For example, some states use our small generator
10 interconnection requirements as a template for distribution
11 level interconnection requirements.

12 So, the area of cybersecurity, is there more that
13 FERC can or should be doing to establish norms that are
14 shared across the federal government and states, question
15 for the panel. If we're perfect, you can tell us that too,
16 that's fine.

17 MR. KJELLANDER: Well, actually this is a good
18 time to say thanks to FERC for some of the things that they
19 put on programs, getting a lot of regulators access to some
20 sensitive information. Over the last three years, I've had
21 a chance to attend three different events in which I had to
22 get security clearances that without the help of the FERC
23 staff, that wouldn't have happened.

24 My takeaway from that though is going forward.
25 We need to recognize that the average tenure of a state

1 commissioner is three and a half years, so none of these
2 efforts can be one and done scenarios, it needs to be
3 ongoing top of the mind and with that perhaps on that same
4 vein is if there was a way to try and create -- I have a
5 very small staff, I live in a very sparsely populated area,
6 there's no one on staff who is super cybersecurity
7 specialist.

8 Would there be a way that a similar program that
9 FERC might be able to work with staff and incorporate them
10 as well because they seem to outlast us to everyone's
11 benefit and that way they've got someone there who knows
12 what the avenues and channels are, has been exposed to this,
13 has maybe a longer, more substantive clearance than some of
14 the one day clearances we've gotten and allows for new
15 commissioners to get that orientation on site and then to
16 know that they need to be involved in some of the things
17 that FERC is working on with the DOE, Homeland Security and
18 others.

19 CHAIRMAN CHATTERJEE: Thank you. We average
20 three and a half years here as well, but that's only because
21 Commissioner LaFleur is 9 years average. With that, I will
22 yield the floor to Secretary Walker.

23 MR. WALKER: Well I'm not nearly as funny as you,
24 so I won't make any jokes. I do want to build off something
25 that Mr. Armstrong said and then this is what concerns me a

1 little bit and I think you're going exactly down the path
2 that I was hopefully we would get which is -- I don't know
3 how many of you were here earlier when OD&I was here, but if
4 you read the 2018 worldwide threat assessment versus the
5 2019 worldwide threat assessment, I think you'll find the
6 two juxtapositions to each other to be very different.

7 And there's a reason for that. We're trying to
8 be very, very forward leaning with regard to making sure
9 where we can't overcome all the clearances that we need to
10 and all those different things that have you know, a myriad
11 of challenges.

12 We can ubiquitously capture and be forthright in
13 what we put forward so that we can let everybody know. And
14 I think you might be able to read where this is going from
15 the standpoint of you know, what we've heard today is what's
16 the cost recovery mechanisms for what we're doing today.

17 And I'm here to tell you what we're doing today
18 is insufficient. Because if it weren't insufficient, we
19 wouldn't be reading the OD&I report suggesting that we have
20 vulnerabilities of a system.

21 Because if we're going to keep going down the
22 same path, one would expect that those reports will get
23 worse and worse. And I think where we're going is and what
24 we need to think about is what happens if we want to really
25 move forward with things like a CRISP Program?

1 Let's say we're working with the EI SAC and NERC,
2 we come up with a much more sophisticated process to go down
3 that. Where does that money come from? Now, clearly
4 obviously, the federal government has got a role, companies
5 have a role, but that's the place where I think we need to
6 focus on, particularly at this hearing Chairman, which I
7 think very astutely was called.

8 Because the status quo does not work. That's why
9 we're having this conversation and the reality is we're
10 going to have, we have many R&D projects, we have lots of
11 work going on with the SCC, we're continuing to evolve the
12 CRISP Program with EI SAC, and NERC to really move forward,
13 but these things are going to take time, effort and money to
14 get in place.

15 And we're going to have to do it quickly, and
16 we're going to have to do it ubiquitously. And so, as this
17 progresses and we come out let's suggest that we come out
18 with a new CRISP Program that costs five times what it does
19 -- what the CRISP Program did when it started. Does that
20 mean that some of the utilities don't participate?

21 I mean obviously we've got a role with the
22 federal government -- I understand that. But if we don't
23 look at how we incentivize certain things that really do
24 have the payback, we're not going to get there.

25 And Mr. Armstrong, you talked about and I want to

1 hear from you -- you talked about the competition component
2 and it sounds like you know, you've got 30,000 miles of
3 system, Transco is a big company, 30% of the U.S. market and
4 so you can lose money and lose -- which I'm not a fan of by
5 the way, lose money and some of these areas because you're
6 making it up in others, right?

7 And that's -- and I understand from a full
8 business model that's fine, but your organization among many
9 of the players here is tremendously important, particularly
10 as the gas pipeline becomes a 30 plus percent contributor to
11 our electric generation.

12 How do we make sure that you are getting your
13 cost recovery? Because I don't want you to wake up in the
14 President's CO one day and say you know what, my ROE's just
15 a little too low, I don't think I'm making this investment.

16 The next thing you know that just cascades
17 through the different players, you know, then Mr. Crane's
18 coming to me and saying oh wait a second, you know, my N
19 minus 2 system I thought I had, well I lose a gas pipeline,
20 I'm going on and doing the frequency load-shedding. So,
21 yeah, I might be N minus 2 on a blue-sky day, but I quickly
22 drop into an under-frequency load-shedding in a blink of an
23 eye. That's what I'd like to hear from you with that in
24 mind, where this is going, how does that impact your
25 recovery scheme?

1 MR. ARMSTRONG: Thank you, well first of all I
2 would say my comment around making sure we know what the
3 threats are is exactly that issue. If there was something
4 bigger that we are not preparing for, we really need to know
5 that and until we understand that, and until the
6 intelligence community really understands what is at risk
7 and what the vulnerabilities are to the systems that in
8 other ways, just like we don't have I would say, complete
9 intelligence about what is going on in that world, I don't
10 think there's complete understanding about really where the
11 points of critical failure are on our systems today by the
12 intelligence community.

13 And bringing that knowledge together in a way
14 that we really can make sure that the investments are
15 prudent and effective, most importantly, rather than
16 spending money on stuff that is not really where our risks
17 are because this isn't going to stop.

18 So, to your point, this is going to continue to
19 snowball I suspect and I think we've got to make sure that
20 we're not spending money that is not effective and to really
21 understanding at a very smart level and not just
22 over-spending broadly, but really narrowly targeting our
23 investments to be effective is what I'm most concerned
24 about.

25 So, I think in terms of the cost recovery issue,

1 I would tell you the biggest issue that I see facing this
2 space right now is that the uncertainty that has come in the
3 regulatory process, whether we like it or not, has been
4 driving the yields up of the equities that support the
5 pipeline industry and that is raising the cost to capital in
6 this space.

7 And you may want to deny that, or you may want to
8 try to drive that lower, but at the end of the day if you
9 deny that, you are going to start to restrict capital
10 available for those kind of investments and I would just
11 suggest that today I think we're in a pretty good spot in
12 terms of covering the costs that are there, but if it does
13 start to escalate we're not going to have the capital
14 available to invest if we get pushed to lower ROE's in the
15 industry and we should all -- and as soon as that risk
16 emerges, it's kind of a death spiral a bit, because as soon
17 as that risk emerges and the investors hear that and they
18 become concerned about the lack of recovery on that, the
19 cost to capital just goes up further.

20 And so I think we've got to make sure that we are
21 measured in terms of how we address it, and I think we've
22 got to make sure that we're looking forward to the size of
23 those capital investments and can predict that and not scare
24 the market because it will become more and more costly to
25 make those investments if we're not careful, thank you.

1 MR. CRANE: Thank you Alan, the point I'm making
2 is a valid point. Answering the question have we been able
3 to recover our cyber and physical security costs to date --
4 yes. But as we start to look at the threat analysis and
5 look at where we're going in the future, understanding a
6 couple of things.

7 One is I pointed out earlier, what is the design
8 basis that we need to have this system designed to so the
9 gas industry, the pipeline industry knows if they want to
10 continue to grow their share of the electric market, what
11 investment needs to be made?

12 What redundancy is required for the northeast
13 corridor and all the gas units that are going on that side
14 of it? So, it starts with the design basis, understanding
15 what the future looks like or what the requirements are for
16 us to design our electric and our gas systems to be able to
17 support that.

18 The interim on that is getting an understanding
19 that we need to have fuel diversification. And for us to be
20 able to maintain the grid with that design basis until we
21 make a transition that has the gas system more reliable and
22 from a redundancy standpoint as we design the electrical
23 system, that's going to be critical going forward.

24 The analysis that we're doing on our electrical
25 systems right now to address the future threats that you've

1 been describing to us in our meetings, we're looking at do
2 we put our own fiber? Communicate only within our own
3 network? Do we disconnect from the internet as much as we
4 can?

5 Do we air gap as much as we can to pull the
6 threats away? What's the expense of that? I did ask our
7 staff to start evaluating it, they looked at me like I was
8 crazy, but we're going --

9 MR. WALKER: Mine does too when I ask them the
10 same thing.

11 MR. CRANE: Yeah, yeah, but we you know, we've
12 got the folks behind us here that are looking at that,
13 working on it to see if we can -- how much more we can
14 minimize it. But if we don't recognize the gas and electric
15 day and the design basis in a holistic manner, we can't
16 ensure that level of reliability.

17 MR. WAILES: You know I don't want to make this
18 too simplistic but one of the things that we need to
19 recognize if we looked at the ramp-up hypothetical that
20 you're referring to, I think we're truly looking at some
21 type of national threat. And at some point, let's figure
22 out at what point would you argue a national defense that we
23 should be funding our own military to support it?

24 So, I think they're -- you know, if you're, as
25 Chris said, there's different things we're doing whether

1 it's fiber or whether it's shielding substations to EMP's
2 that our costs that we're looking at incurring internally,
3 but at some point if there's a system that's being developed
4 that's hypothetically five times more expensive than CRISP,
5 but does all sorts of other stuff as we know, there's things
6 in play.

7 I'm not so sure that those are not national
8 prerogatives, that's not a part of a national defense that
9 doesn't have to be looked at, covered that way, rather than
10 try to have it -- because there may not be any way to social
11 that. If you have a utility our size trying to cover the
12 fixed costs associated with CRISP as identified by Nick,
13 compared to a utility the size of Chris, well that's a
14 dramatic difference.

15 So, I'm not so sure you don't have to step back
16 and say we know where these threats are. Some of them we
17 have an obligation to take care of as we normally would with
18 respect to reliability, some of them are national
19 emergencies, so are national threat affected, so a thought.

20 MR. EMLER: As I mentioned in my remarks, the
21 Fusion Center is a strategic plan and by strategic, I mean
22 it looks down the road. What is it that it can help the
23 companies do to plan for the future?

24 Not meaning to insult anybody, but the
25 intelligence community doesn't know what the intelligence

1 community doesn't know. They are not all utility operators.
2 They know the intel, but they don't know how that threat
3 affects the utility. That's why in my comments I said the
4 utilities need more staff that have clearances so that they
5 can look at the threat and say this threat affects my
6 company this way and from a strategic standpoint, this is
7 what we need to look at doing in the future, sorry I don't
8 mean to say future computer.

9 So, it's not a tactical solution. It is a
10 strategic solution for future planning.

11 MR. WALKER: And so, I do want to add one comment
12 with regard to the IC and the OD&I report. So, for anything
13 to end up in that report there basically had to be consensus
14 among the 16 agencies that are the intelligence community of
15 which DOE is one of.

16 So, you can well imagine to get 16 federal
17 agencies to agree on a statement means that there's some
18 level of confidence with it. So, the other piece I wanted
19 to go down the path of and Chris, you just mentioned with
20 the fiber and it's something we've been looking at.

21 And with regard to the Fusion Center, I just want
22 to point out -- so, the IC community does have some
23 visibility and understanding of how utilities work because
24 we have the three PMA's that are transmission utilities now.

25 Obviously, they don't run it day-to-day, we're

1 very fortunate to have some very talented people on the
2 PMA's actually run it, but they do have some insight. One
3 of the areas that's become a linchpin or an Achilles heel
4 potentially, as we look across the landscape and as we
5 talked to the ESCC, is the com's piece -- the
6 communication, particularly as it relates to communication
7 within operating the network.

8 And that refers to the GPS for the PMUs that are
9 in place for you know, running the transmission system as
10 well as just the general comments from you know, efficiency
11 and effectiveness standpoint.

12 And I heard a couple of people say that we don't
13 have, or you don't have jurisdiction over the telecom
14 component within your jurisdiction. So, with regard to the
15 cyber aspects recognized just yesterday we had received a
16 notice from NERC that we were going -- we were concerned
17 about two Chinese companies while waiting DT, and the
18 vulnerabilities that reside in that -- those systems.

19 At DOE we ceased the utilization of those pieces
20 of equipment just last week, very affirmatively across all
21 national labs, all of our PMA's and every other facility
22 within DOE. So, as we look at the com's piece which you
23 don't have jurisdiction over, how will we look at that from
24 a recovery standpoint or a security's standpoint since you
25 don't have jurisdiction, it's a recovery mechanism that

1 obviously any of your facilities or any utilities that you
2 have would be seeking recovery.

3 This cloud-based technology, you know, I've heard
4 this argument from some of the major utilities in the United
5 States that it's considered an O&M expense, it may not even
6 qualify for being acceptable in the first place.

7 I will highlight that we used cloud technology
8 within the federal government pretty extensively so I'm not
9 sure what the concern is obviously. There are limitations
10 on what you can do or not do, but there are capabilities
11 within that technology.

12 So, where does the com's piece fit into -- I mean
13 it's an integral part of your company's systems, but where
14 does that fit into the regulatory model and into the
15 recovery component and from a location that perhaps should
16 be incentivized?

17 I think, Chris, you pointed out the
18 point-to-point and we're doing a lot of work in this space
19 that fundamentally eliminates some of the cyber risk if it
20 can be done, but there's some tremendous gaps in fiber
21 across the United States, I'd like your thoughts on that
22 maybe Jay?

23 MR. EMLER: I can tell you that I have personally
24 met with most of the telecom representatives in Kansas to
25 talk about the very issue. One of them said that well,

1 we're not really connected to anything that would be
2 troublesome and I simply said, "Do you get email?"

3 And he said, "Well yeah sure." So, even -- but I
4 don't regulate it. I can't force him to do anything with
5 this small company, he can't afford to do a lot. I
6 understand that, but he doesn't seem to grasp the bigger
7 picture about how integral he is to the entire network.

8 So, I have personally met with them. I have
9 talked with them about -- at a high level, about their
10 security measures and what they're willing to do. One of
11 their problems for example, with working with the Fusion
12 Center, is simply that they are small companies. They can't
13 afford to have somebody on their staff that's cleared and
14 running their data, be at the Fusion Center all the time.

15 Well, that's one of the reasons that the KCC
16 funds a position at the Fusion Center to help utilities, but
17 they still have to have somebody that they can talk to at
18 the local company and when it's a small company like that,
19 there isn't anybody to talk to.

20 So, it's a problem, it's a problem for us because
21 we can't mandate it. It's a problem for them because they
22 really don't know what they don't know and they think that
23 because software protection mechanism is sufficient for
24 their system, so it's difficult for us to require them to do
25 much of anything, but we try and educate them to what they

1 need to be doing.

2 Again, it's not much that we can do other than
3 try and help them understand that they are the open door.

4 MR. WALKER: I guess we could advocate for the
5 utilities to actually own their com's piece.

6 MR. EMLER: Could -- but.

7 MR. WALKER: Possible.

8 MR. EMLER: But could they afford that?

9 MR. WALKER: I mean and those are the things
10 we're talking about, right? And so, I think again, as we
11 move forward, as we get more sophisticated in understanding
12 the threat and coming up with solutions toward it, those are
13 options I think that may be on the table, right, yes?

14 MR. KJELLANDER: You brought up the idea that
15 yeah, we've heard a lot about is do you rate base the cloud?
16 And historically as regulators, if you actually own the
17 physical box -- the server and the software, then that could
18 go under rate base and the question we're going to have to
19 deal with in sort of a changing environment is that now that
20 it's moving to more cloud-based, if it does the same
21 function, why shouldn't they get the same treatment?

22 Especially if I'm making the same investment?
23 And that's something that I think, we as regulators are
24 going to have to try to get our heads around and our arms
25 around because it's going to require us to think about

1 something a little differently than perhaps, we have
2 historically over the last hundred years.

3 MR. WALKER: Like a virtual rate base?

4 MR. KJELLANDER: There you have it, virtual, when
5 I was a regulatory attorney.

6 MR. WALKER: Virtual customers will pay for that
7 rate in a virtual return, touche. I yield back to the
8 Chairman, thank you Paul.

9 CHAIRMAN CHATTERJEE: Thank you Secretary Walker.
10 I thought you were very funny.

11 COMMISSIONER LAFLEUR: Thank you very much. I
12 think this has been an interesting discussion on a lot of
13 fronts. I particularly appreciated the thorough discussion
14 of rate recovery. It seems like there's been an urban
15 legend that I've heard a lot that somehow the NERC standards
16 are a barrier to people recovering all the money they need
17 to because they -- you can only get the money for what's in
18 the standards and not beyond.

19 And I've said numerous times at various events,
20 you know, how can that be with formula rates and so forth,
21 if anyone is having a problem come see me after the meeting.
22 I need to know, and sometimes that just ended it because no
23 one has ever come see me, but other times people say well,
24 you know, it's the states.

25 It's the states because we have to go through the

1 states, and that certainly doesn't seem to be the case in
2 Kansas, Idaho or New Jersey because you've given very
3 thorough explanations of how you look at it, but I know
4 there will be an opportunity for comment after the Tech
5 Conference if there's something we're missing here, but it's
6 been just very helpful to really understand how cyber
7 investments go through state rates.

8 I want to probe a little bit more on another
9 aspect -- an aspect of federal/state cooperation. Because
10 of the fact that the networks we regulate and the networks
11 you regulate are connected, and particularly with all of the
12 things at the -- in the distribution network starting to
13 come together to be virtual wholesale resources in the
14 future with all the distributed resources, I've frequently
15 and I've been told by saying speeches that oh, there's going
16 to have to be such close cooperation between the federal and
17 state government, oh yes, that's true.

18 But what does that really look like? Because
19 what I really heard from the states, just as we heard today,
20 9 times out of 10 they mentioned it was really useful when
21 Joe McClelland set up a briefing and we got our clearances,
22 and we got to hear from the FBI or whatever.

23 That was really useful and that's great, that's
24 the convening authority if we can help that's wonderful.
25 But I meant really like should we be working on how do you

1 view your supply chain? How do we do our supply chain? Are
2 there best practices? Should we be conforming anything?

3 And I'm interested first of all if you think
4 there's a need for that, if it would be helpful and if it
5 would any ideas? I know Paul had some ideas in his
6 testimony that you already mentioned on involving the staff
7 more because of their more enduring rule, but I mean should
8 we be using getting more federal participation in the
9 NARUC's critical infrastructure subcommittee at the staff
10 level, or even more a member, but actually more day-to-day
11 participation at the Commissioner level? Or should we set
12 up some other working group or is there some other one of
13 the alphabet soup of all the things we do together that we
14 could somehow task with this?

15 Or is it not a thing? Because I feel like I'm
16 just saying a lot of words, and it doesn't feel like we're
17 really actually comparing practices together in a real way.
18 So, I'm interested from any of the state folks first what
19 you think.

20 MR. KJELLANDER: It's a thing. And we do need to
21 do a lot of what you described. You hit it on the head as
22 we're not quite sure what to do and I think one of the
23 concerns we have is are we trying to reinvent the wheel?
24 Are we replicating something that's going on somewhere else
25 because we often find that we are?

1 But I think you mentioned the critical
2 infrastructure committee within NARUC and the role that FERC
3 has played with our National Association and I think to the
4 extent that we can raise those questions in that forum, it
5 gives us the opportunity to build on what we've done.

6 And I mentioned this earlier -- my fear is that
7 we create these reports and documents, we set them on a
8 shelf, and we don't recognize that they need to be living
9 documents because this is constantly evolving.
10 Additionally, if there was some way to have some benchmark
11 at what some of the prices might be for some of the
12 technology and software providers, and which ones are
13 actually the ones we should be dealing with and staying away
14 from.

15 If there was some way to get better access to
16 that as regulators. To understand what the range of prices
17 might be, recognizing that one size doesn't fit all. Have
18 you been having that discussion as to why one size doesn't
19 fit all?

20 Because when I look at the three major electric
21 utilities that I regulate, if all of them bought the same
22 type of solution to resolve some of their cybersecurity
23 issues, they would all come in with three every different
24 cost recovery expenses because the utilities are very
25 different, with different resource stacks or distribution of

1 transmission systems are very different, even working with
2 the same vendors in order to get the patches they need to
3 work within their system, is going to cost them more for
4 that.

5 We need to understand that and recognize that
6 hey, they spent this much on XYZ software, they spent this
7 much, they spent that much, they spent 2 million, 4 million,
8 6 million -- the right answer's 3 million? That's not the
9 way we should go about it.

10 But I think we need to find ways in which we can
11 have that dialogue that just sort of fair through those
12 issues and I think you hit wisely that I think we do have
13 the structure in place and we need to continue working on
14 the cooperative federalism so that maybe we know what that
15 actually means at the end of the day too.

16 MR. CHIVUKULA: Commissioner, one of the things,
17 one of the utilities in New Jersey came to me and talked
18 about some of the internet of things, IOTs, and they said
19 they're going to be duality, I don't know how many billions
20 are already there, so that introduces additional risk into
21 the network -- this situation network.

22 And as I understand low standards for this IOT
23 devices. California recently passed a law regarding IOT
24 standard. I think federal government should look at how can
25 we -- these are additional risks that we have to deal with

1 the points of entry and how do we do this and come up with
2 some standards and help us out?

3 COMMISSIONER LAFLEUR: Is NIST doing something?
4 I hate to add more alphabet soup here, but I thought NIST
5 had -- National Institute for Standard Technology had some
6 kind of smart grid standards, but yeah?

7 MR. CHIVUKULA: Right, I think California
8 recently passed a law because IOT's don't have any --
9 because the fiber IOT manufacturer and they're low
10 standards. I just make -- there is not security
11 protections on that device.

12 Of course, because it adds additional cost to
13 that, so something to look at. One other point I just want
14 to make is that the Chairman asked earlier, you know, how
15 the federal government and FERC can help us. So, when
16 you're doing the formula base rate making or adding some
17 incentives, make sure that it's evidence-based.

18 And there is some kind of a cost to benefit
19 analysis is done and also you need to have measurement and
20 verification because giving money is one thing, making sure
21 that is indeed getting done because we had a -- you're not
22 in front of the rate-payers, we are in front of the
23 rate-payers.

24 In New Jersey we pay very high rates for
25 electricity and so we want to make sure that whatever you

1 are doing, your actions are impacting the rate-payer and we
2 are answering to them, so please help us, so.

3 MR. EMLER: I guess Commissioner, I would say
4 that education is always a good thing to the extent that
5 FERC could be involved with especially educating as the
6 Commissioner said, staff. Keeping them apprised of the
7 global picture of things as you can would be extremely
8 helpful.

9 I think you're going to run into a little
10 opposition from states if they think you're getting a little
11 too involved. Not that they're independent --

12 COMMISSIONER LAFLEUR: It was said at the last
13 couple critical infrastructure meetings when the resolutions
14 have been tabled, they weren't my resolutions, but I could
15 just tell there was tension.

16 MR. EMLER: You know, we're gosh darn independent
17 for a reason. We're out in the states and especially when
18 you come from a rural state, you don't need nobody back east
19 telling you what to do.

20 But you do need some help knowing what the right
21 things to do are and so I think to the extent that you can
22 remain involved with NARUC and the critical infrastructure
23 committee and in other areas as well, that would be
24 beneficial.

25 COMMISSIONER LAFLEUR: Well, I would just say as

1 the NARUC meetings just seem to come up as soon as you've
2 had one, the next one is on your horizon. If there are
3 topics you want, either at the critical infrastructure, or
4 the critical infrastructure staff committee, or you want
5 engagement, I know there's been engagement in the past, the
6 more notice and the more specific you can be so we can try -
7 - and not just kind of go to critical infrastructure and
8 have another conversation about like, "Hey, I'd really like
9 to work with you. I'd also really like to work with you,"
10 and then not see them until the next NARUC, which seems to
11 be sometimes my pattern, and I just want to make sure we're
12 really doing something.

13 I -- just the topic on staff training brings me
14 to the last question I wanted to ask. We talked a lot about
15 what equipment you put in, what fiber optics, you know, N
16 minus 1, N minus 2, N minus 15, someone said in the last
17 panel, but one of the things we read all the time and we
18 heard in the last panel is a lot of these cyber issues are
19 simple human or at least facilitated by simple human
20 mistakes -- lack of cultural awareness of the importance of
21 your password protection and all the other things,
22 submitting, turning -- giving into a spear phishing attack,
23 and human error in different ways.

24 And a lot of the attacks are internal, all of the
25 things we've all read and heard. So, we have three CEO's

1 and then all these states, is there anything more that the
2 federal government can help with on training, or how are we
3 approaching the human side of this in your companies and
4 collectively, is there something we should be doing because
5 that's our best -- one of our best defenses as well as all
6 of the things you buy at the computer store.

7 I know there's no computer store, but however you
8 buy it.

9 MR. WAILES: I guess I would comment on that. It
10 seems to be that I think, most of us recognize actually the
11 least expensive thing you can do is cyber hygiene and
12 keeping it front of everybody in the organization.

13 We treat it just like safety. If we're having
14 general meetings, we talk about it just like we talk about
15 safety. I don't see that there is an overarching role and a
16 regulatory perspective for that, but I do think if there is
17 one in continued education and pushing it, which we do -- we
18 even talk, in Nebraska you might guess I think there's 160
19 public power utilities, most of them are very small.

20 I have spoke to the Nebraska League of Cities and
21 actually that's the kind of thing you push and then we
22 provide support for them in some of that too. We also do a
23 lot of creative things. I think everybody does phishing
24 tests, and we all know that there's some company you want to
25 use for that and some of you don't.

1 But the, you know, there's a whole host of things
2 in that that are very inexpensive and so, you know, I think
3 that you can do clever things, you can do lots of things,
4 there's a lot of resources out there. You know, utilities
5 can go to trade associations and get that support, but I
6 don't see a regulatory I guess, place for that.

7 COMMISSIONER LAFLEUR: Well, in general the
8 electric industry is very good at safety although sometimes
9 obsessed with electrical safety as opposed to all the other
10 and by the way I just want to say this -- four CEO's, I'm
11 not a math major.

12 MR. CRANE: The -- I think the scale of the
13 company makes a little bit of difference in the resources
14 available to continue to sensitize train. You know we do
15 the testing, the phishing testing now, and we hold
16 individuals accountable. We track the habitual clickers.

17 There's a lot of things that we can do and do do.
18 I think I don't know what venue would come out of its NERC
19 or FERC but sharing best practices with the smaller entities
20 might be a support.

21 Back to your previous question just real-quick.
22 Education -- the com's issue is a huge issue. And having
23 the state regulators more informed of the vulnerabilities
24 there and what we may be coming to them to say to do. We
25 have some interconnection on old twisted pairs and so wee

1 know that they don't want to maintain those anymore.

2 Having the ability to have fiber at all the
3 critical you know, what kind of return are the com's going
4 to get on that fiber going in, versus us being able to put
5 it in under a rate-based mechanism?

6 The -- we've done testing at three of our
7 utilities and we're going to continue on, where we're
8 actually taking the SCATA system off of the main frame, and
9 putting it in a manual mode and dispatching people and
10 figuring out where the communications glitches are where we
11 can't see what's going on so we can start to get that much
12 more secure.

13 If there's something going on nationwide and it
14 hasn't hit us yet, how do we switch off and be able to
15 operate the system and train the operators? But if being
16 independent and credible with the regulators as you are,
17 being able to help continue that communications would be
18 critical.

19 COMMISSIONER GLICK: Thanks Mr. Chairman. So,
20 it's pretty clear that the headline from today, at least
21 from this particular panel is that there just aren't any --
22 that the cost recovery at the state or federal level really
23 isn't a barrier to utilities doing what they need to do to
24 protect, you know, at least from physical or cyberattacks, I
25 think that's pretty clear. I kind of was thinking through

1 the discussion that's going on, maybe the better approach
2 might have been to have a Technical Conference to consider
3 what utilities should be doing that they're not doing to
4 address the threat that Secretary Walker and others referred
5 to and Director Coats had outlined to the Senate
6 Intelligence Committee.

7 I think that's a relevant issue, it's a serious
8 issue we need to consider. Now maybe we couldn't have had
9 that discussion out in the open I don't know, but I think we
10 need to think more about that and not necessarily think of
11 barriers that may not be there.

12 I would say that on CRISP, Mr. Chivukula, I
13 wanted to get your point on CRISP because I think it's a
14 good one. I've been hearing for years how successful and
15 effective and important that program is -- participating in
16 that program is to cybersecurity and meanwhile a lot of
17 utilities aren't participating, especially the smaller ones
18 because they can't afford it.

19 And so here we are saying it's very important
20 they have to comply with cyber rules, it's very important
21 that you make sure your system is cyber secure, but you're
22 not participating in a program that we know is effective to
23 addressing it.

24 So, I think, you know, this isn't really for
25 FERC, it's really more for Congress and maybe the Department

1 of Energy and others, but we need to figure out a way that's
2 going to ensure that everybody participates in CRISP and if
3 there's some way to share the funding of that and maybe we
4 have a slight role in that, but something needs to be done
5 because it's -- I think it's criminal in a lot of ways not
6 to have all members participating in what is clearly a
7 successful program.

8 Mr. Armstrong, I wanted to touch base with you.
9 I, you know, I thought I was going to address gas pipeline
10 cybersecurity and I'll do that one more time, but I want to
11 get at a slightly different perspective.

12 So, you know, because I spoke to Mr. -- to Don
13 Santa about this before in the first panel because I read
14 your testimony as well as his and I was interested in, you
15 know, because a lot of gas pipelines as you pointed out,
16 have negotiated rates and others have competitively set
17 rates and so there's not a guarantee that you can recover
18 your costs as opposed to your traditional cost to service
19 rate making.

20 And so, I was kind of interested that you and he
21 had taken a position that outside of the policy statement
22 that the Commission issued right after 911, we really don't
23 need to do anything else. And I got to thinking about it a
24 little bit and you know, you referred to this earlier, there
25 are certainly competitive pressures that you are under and

1 I'm assuming that that's the issue, right?

2 In the sense that you might -- if you incurred
3 that expense, your competitors -- the other pipeline
4 companies that you're competing with may not be incurring
5 that expense and therefore you can't incur that expense
6 without losing customers.

7 And so, I'm wondering if there's and maybe going
8 back to the question I had earlier, the TSA is maybe if
9 those expenses are important and are essential that we
10 again, insure that everyone -- all pipelines make that,
11 incur that expense essentially make that expenditure. I was
12 curious what you thought about that.

13 MR. ARMSTRONG: Well I would just say from my
14 knowledge, and I'll be the first to admit that I don't have
15 the detailed knowledge of how all of the pipeline operators
16 -- I can say within INGA that there is a commitment within
17 the INGA members to comply with like the TSA guidelines and
18 so forth.

19 So, speaking to the INGA membership, I think I
20 can say very comfortably that people are making those
21 investments today as required to protect the systems and
22 that the isolation and the redundancy of the system are
23 working very quickly. Please don't misunderstand, we are
24 constantly under attack. Everybody's systems are constantly
25 under attack and we all know that.

1 But to date, I would say we've invested
2 adequately to accomplish that as my conversation with
3 Secretary Walker on that issue. We really need to be
4 thinking forward and thinking proactively, and that's where
5 we may get into a completely different realm that the
6 competitive nature of the space and the pressure on the
7 ROE's from the investor community matched up with the
8 pressure from the FERC and any other utility commissions,
9 downward pressure on that may start to cause a problem.

10 So, you know, looking forward basis I think we
11 very much need to keep our eyes wide open as to that issue
12 but I will say that in the current environment, I'm not
13 aware of where there is an adequate investment going on and
14 people are protecting it.

15 Remember that losing the through put on the
16 systems is something that folks can't afford either. So,
17 from a revenue standpoint, so it's not like we're not
18 aligned with making sure that we keep our systems reliable
19 as well.

20 And many of these systems are integrated back
21 into our unregulated systems as well and so we're dependent
22 on two sources of revenue with that. So, I would just say
23 today I don't see a problem, I think it's very -- I think
24 what you all are studying is spot on to the kind of things
25 you should be, and I think thinking about it proactively,

1 about where expenses may go and making sure you have a
2 mechanism that's effective in a competitive environment to
3 recover that is exactly what the Commission ought to be
4 thinking about right now.

5 COMMISSIONER GLICK: Just one last question and
6 you had just referenced the fact that all INGA members --
7 all INGA members are following the TSA guidelines which is
8 great. I think it's important to note, and this is what I
9 kind of wanted to get to, it's important to note that not
10 all major pipeline companies are INGA members and some of
11 them have track records, at least in regard to safety -- I
12 don't want to get to cybersecurity but we'll do safety, a
13 track record that may not be as stellar as Williams or some
14 of the other companies that are members of INGA.

15 And you mentioned you were talking about the
16 Transco Houston control center incident and I think, you
17 know, to your credit you had the redundancies and you had
18 everything set up, you were able to switch over very quickly
19 and address the situation without any disruption to service.

20 But we know that some companies don't necessarily
21 -- sometimes they might cut corners. They may not have that
22 same type of redundancy. So, how do we address that without
23 those types of conflicts without imposing mandatory
24 standards on everybody?

25 MR. ARMSTRONG: Yeah again, the main thing I

1 would start with there, and I'm not answering the question
2 around how you solve, you know, that particular issue
3 necessarily, but I would say you better be focused on what
4 the right solutions are and really where the
5 vulnerabilities are first.

6 And from my vantage point, we have learned still,
7 even within the framework we have today, we have plenty of
8 room for improvement by identifying what the risks really
9 are and what the vulnerabilities really area and working on
10 that.

11 If we identify that and we say that is so big
12 that we have to insist on these other methods, then that's a
13 different -- that's not in the first nine innings, that's in
14 the double-header. And so, I would just say I think we need
15 to decide what we're up against first before we solve a
16 problem that's not here relative to the current cost and the
17 current cost structure. I don't think there's major issues
18 to be resolved.

19 If it becomes a bigger issue then I think it
20 needs to be solved across the industry, not just with those
21 you know, potential folks on the edge, non-operating, thank
22 you.

23 COMMISSIONER GLICK: Thank you very much.

24 MR. BROWN: Commissioner, I might add in terms of
25 asking, you know, what's next. One of the things I was

1 going to speak about earlier was the security posture that
2 we have, knowing where we are relative to something.

3 There are cyber maturity models -- numerous of
4 those that have been developed over the last few years.
5 There's nothing mandatory about utilizing these models, but
6 last year we undertook internally looking at evaluating
7 those different models, choosing a particular model that we
8 thought was most relevant to our organization.

9 And then assessing our current posture relative
10 to that model. Not only did we do an internal assessment
11 against that model, we hired an independent contractor to
12 come in and assess as not only against the model we had
13 selected, but against the model that this consultant used as
14 across any number of industries.

15 Then once we knew where we were relative to that
16 model, the question we asked ourselves is where, do we
17 believe we really need to be relative to the risks that we
18 face from a corporate perspective.

19 And from that then we put together -- I think, a
20 very well developed and thought out long-term strategic plan
21 to get us to where we believe we need to be. If you don't
22 go through that kind of thought process, and you're going to
23 be kind of chasing your tail.

24 You don't know where you are relative to any
25 particular standard and you don't know where the investments

1 need to be and the value of those investments. And I will
2 tell you it's not a once and done thing because every single
3 time a new threat comes up, where you are in that relative
4 ranking in the model, in multiple categories in that model
5 changes.

6 So, I will tell you the larger companies that
7 have very robust risk management programs have gone through
8 that. Many of our 97 members have not gone through that
9 kind of step. It's not a required step. It's not an
10 expensive step.

11 It will take time and it will take honesty in
12 terms if you only use a self-assessment, but I was very
13 pleased when we went through that and it's that type of
14 security posturing that is needed to take us above and
15 beyond the standards.

16 The standards are foundational and they're only
17 foundational. Security goes way above that and we need to
18 focus on that.

19 COMMISSIONER GLICK: If your members, if they're
20 not expensive, why are some of your members not engaged in
21 that process?

22 MR. BROWN: So, a lot don't know about it. And I
23 will tell you where I learned about those models was from a
24 different industry. And they're beginning to develop and
25 they're beginning to proliferate the challenges as now there

1 are so many models, how do you choose which one to use?

2 COMMISSIONER GLICK: Thank you very much.

3 MR. WAILES: Commissioner, one of the things I
4 mentioned was the deal, the cooperative agreement with APPA.
5 In fact, the tools used for that to use for smarter
6 utilities was based on the C2M2 model the DOE has and then
7 use that as basically to come up with a baseline and then
8 let utilities transition as Nick said, as they got better
9 then they could move on to these other assessment tools.

10 So, in fact that is a good example of where
11 funding from DOE on a programmatic basis was spreading
12 basically a better environment for security.

13 MR. EMLER: Since they mentioned C2M2, I had gone
14 back to after our meeting where I looked at the C2M2 model.
15 I went back and suggested to Commission staff that they get
16 with our jurisdictional utilities and ask them to do the
17 C2M2, and frankly we met a lot of opposition to that.

18 We didn't make it mandatory -- at least not yet.
19 Probably won't during my tenure since it's so short, but
20 it's still something that staff is at least got on its plate
21 to take a look at, trying to get the Commission to say okay,
22 you have to pick whether it's the C2M2 model or not, you
23 have to pick a model and show us where you're at.

24 So, I think Commissions may need to at some
25 point, make it a requirement that that very thing be done.

1 COMMISSIONER MCNAMEE: Thank you. I want to
2 address the issue -- I think we miss something if we think
3 that cost recovery is not an issue and that's because of
4 what Assistant Secretary Walker brought up which is that
5 they're things that are out there that maybe aren't being
6 invested in.

7 And when I think about when I've done rate cases,
8 I've talked to companies. You know the issue is allocation
9 of capital. There's only so much capital that can be
10 allocated. The company makes a five-year plan, a one-year
11 plan, and then everybody competes to see how much of the pie
12 can they get and allocate.

13 And it seems that there's always going to be
14 minimal amounts of work that you can do on cybersecurity and
15 you're going to invest in that. The question is -- is there
16 more that can be done? And I think that's part of the
17 reason for this panel for cost recovery and incentives.

18 And I guess what I want to know is some
19 perspective about is cost recovery as is currently
20 structured, is it giving the right incentives for the
21 companies to invest? Should they be seeing that they can
22 get a better return if they do a little bit more in cyber
23 security or is just the way things are is that just
24 sufficient? Is the minimum enough? Any thoughts on that?

25 MR. CRANE: I do. The -- when we answered that

1 cyber hasn't specifically or physical specifically an issue
2 with recovery, we do have jurisdictions that have
3 significant lag. And it's overall on the investment so what
4 we're working on in almost every one of our jurisdictions,
5 is to suggest alternate rate-making that would take that lag
6 out.

7 Our Illinois utility Con-Ed is an under a formula
8 rate. There is no issue besides the management of the
9 capital to address the reliability and the cyber issues --
10 that's how we throttle it, not capital being available.

11 But being able to work within the states --
12 proceedings in Maryland, proceedings in D.C., we just went
13 through a proceeding in New Jersey. We finished a
14 proceeding in Delaware and we just got one in Pennsylvania
15 to allow -- to have the regulators recognize the
16 investments that we have to make, but the lag is
17 unacceptable and is the limiting factor.

18 If you're a utility with a 5% ROE, you have
19 investors asking you why are you putting so much money into
20 it? So, our overarching issue is get the right regulatory
21 recovery mechanism for the prudent investments and the cyber
22 issues are -- cyber and physical, are the number one
23 priority for capital. You do not want to lose Chicago or
24 D.C. or Baltimore in some long-term outage. So, just to
25 frame it in a different way.

1 MR. KJELLANDER: What you're talking about might
2 fit within sort of the structure of a performance-based
3 regulatory process. And I'm not as familiar with them. I
4 don't utilize those in our state, there are other
5 commissions that have. The only problem I have trying to
6 get my head wrapped around a performance-based component for
7 cybersecurity expenses is how do you set the benchmark for
8 that?

9 And that's the problem that I kind of have if
10 you're trying to look at it as an incentive beyond. Do you
11 set it too low? Do you set it too high? And where you set
12 that and the factors that you put into that can really
13 almost be a disincentive to additional investment beyond
14 that depending on how you structure it.

15 So, that would be the only question I would have,
16 that I would want to try to understand more someone
17 proposing it in our forum, is just how do we set a benchmark
18 for that minimum performance level that they have to do
19 better than, and what assurances can we have that we've set
20 it appropriately?

21 And it's a good question, I don't know the
22 answer.

23 MR. EMLER: I think as I mentioned in my remarks
24 that there are different ways for a company to secure
25 payment for making security investments. That's one of the

1 reasons we have the O&M rider because the regulatory lag
2 that was mentioned, we have two utilities that now are on a
3 five-year moratorium on their base rates.

4 That was part of a negotiated settlement. So, if
5 they need to spend significant amounts on security measures,
6 they're probably going to have to look at coming in for a
7 surcharge. They're not going to want to wait five years
8 until they can roll it into their base rates.

9 So, I think the biggest drawback for spending --
10 for a utility spending more than just the bare minimum is
11 the big issue of regulatory lag and how do we get the
12 appropriate amount of money back?

13 The big issue for the Commission is, okay,
14 explain to me why this is really necessary. What is it --
15 what threat are you trying to combat and why do you need to
16 spend this much money on it?

17 And there isn't a lot of education as you've
18 heard from I think all of us. There isn't a lot of
19 education out there for us to know what is the right thing?
20 What is the right benchmark to look against? And so that's
21 the difficult decision that we state regulators have and our
22 staffs have.

23 MR. ARMSTRONG: I would just -- I think you're
24 spot on with, you know, your concern around the capital
25 allocation program that goes on and I think you described

1 the process and a lot of corporations very well.

2 And so, I do think that we -- as I stated
3 earlier, we do need to make sure that the return is not so
4 low that it's a disincentive against the other capital
5 investment opportunities with the company and so I think it
6 is generally understood that they've done a good job of
7 managing that.

8 But again, as we think proactively, you are not
9 going to attract, under the current model and I'll just
10 speak for Williams for a moment. You're not going to
11 attract proactive dollars in to going out and getting ahead
12 of the curve on something we're not even sure what we're
13 defending against, if we're not informed on what we're
14 defending against, we're not going to get proactive dollars
15 attracted to that.

16 The current ROE's allowed within the pipeline
17 space that we have today so, just to be very blunt about
18 that and I would say we're as well positioned as anybody,
19 you know, within the space within the gas pipelines to do
20 that.

21 So, I do think that that is certainly a concern
22 but again, I think our focus right now should be on this
23 convergence of knowledge between intelligence and between
24 the operations of the systems is really where our focus
25 should be right now, thank you.

1 COMMISSIONER MCNAMEE: This is more of a
2 practical question for the State Commissioners. But have
3 you all seen any issues on cost allocation? Usually in a
4 rate case you get a fight between the residential, the
5 commercials and the industrials about you know, how the
6 costs should be allocated.

7 Not that it's easy, but usually you can identify
8 it by you know, what's your consumption and everything, but
9 because the way that security issues can affect everybody,
10 have you all seen any battles or see any issues coming up
11 with cost allocation between different customer classes?

12 MR. EMLER: Well as you mentioned, there's always
13 a battle over cost allocation. I have not, in any of the
14 rate cases that I have participated in over the last five
15 years, there has never been an issue about security
16 discussed with the Commissioners.

17 There may have been with staff, but it's never
18 come to fruition.

19 MR. KJELLANDER: Commissioner, we haven't yet
20 seen that and again I'll echo that we always have arguments
21 over cost allocation. Those are the ones I like to leave
22 the room on if I can.

23 But part of the reason that I think we're not is
24 just when we dealt -- at least in more recent rate cases,
25 the cybersecurity costs, a lot of it were embedded into some

1 of the other expenses and aren't actually identified as
2 cybersecurity expenses for a lot of realistic reasons.

3 And also, we haven't seen there be such a huge
4 swing from one rate case to the next in terms of costs that
5 might go to security. Now when we see that, we may be
6 hearing some more arguments over that going forward but
7 today we haven't seen that huge change in costs.

8 There's a chance we could and that will clearly
9 be an issue, but I think too, the point that was made that I
10 don't think there's anyone, the industrial customers and
11 others that don't recognize the significance that security
12 because if we miss the mark, they're the ones that suffer.

13 I have one company that their load is 200
14 megawatts, they care, and they notice real-quick.

15 COMMISSIONER MCNAMEE: My last question is really
16 related to prudence. You know, gold-plating is always a
17 problem. We talked about it, the threat can be demonstrated
18 then to recovery of the authorized, but in this environment
19 it sounds like it's a lot different than saying the loads
20 growing, we've got to you know, meet that new load and you
21 know, here's the new thing that we need to build, we need to
22 buy or here's the trucks we need to buy.

23 This is kind of we think there's something out
24 there, we've been told there might be something out there,
25 and there may be something we need to invest in today for

1 something we don't even know about tomorrow.

2 So, how should we all, how should you all think
3 about prudence in those issues? Is there a new paradigm we
4 need to think about in terms of prudence?

5 MR. BROWN: Well for one, I think that's where
6 the cyber maturing models can come in. I mean it's pretty
7 easy to go through those questions and steps and you know,
8 while there's maybe some subjectivity when you put tons of
9 our staff in the room and looking through that, quite
10 frankly, I was very pleased that we were harder on ourselves
11 than the third party consultant was on the model that we had
12 selected.

13 But again, that's one of the reasons that I
14 believed going through that process was so very important
15 because I have to defend my costs to our 97 members and 130
16 plus customers all the time. And how much do you spend on
17 cybersecurity? I mean it could be never-ending and
18 certainly we don't want a gold plate, but I want to feel
19 like we're making prudent decisions based on managing risk -
20 - corporate risk.

21 And as I stated earlier, it is absolutely our
22 single highest risk and I imagine it is for many of the
23 utilities.

24 MR. WAILES: One of the comments I made earlier
25 was with respect to how important information sharing was as

1 it related to being able to determine those kinds of
2 investments and feel good about them. And if you look back
3 at the original parts of the SCC when it was formed up, part
4 of that was to get CEOs in the room with clearances in order
5 to be able to get information that was not otherwise
6 available and to get more of that -- those clearances out in
7 the industry as well.

8 Part of that was obviously, you couldn't go back
9 and tell anybody about what you knew, but that your Board
10 would have enough faith in you as well as your staff you say
11 no, we need to do these things.

12 And I know that sounds like it's a little
13 elusive, but we are dealing with something that the industry
14 ten years ago didn't think we'd be dealing with and I think
15 that's the solution in part, is to make sure as much as we
16 can, as hard as our government partners work to be able to
17 communicate things that they declassify as far as they can.

18 There's still other information out there that
19 can make you be worried and you had some of that on the
20 earlier panel this morning when they're talking about you
21 know, from D&I, just basically here's things, trust us,
22 we've got all these people and the more you learned about
23 that the more you can say yeah, we really need to make these
24 investments.

25 Closing Remarks:

1 CHAIRMAN CHATTERJEE: Thank you again to all of
2 our panelists for an outstanding discussion. Thanks to my
3 colleagues for a great day. I think we got a lot of rich
4 dialogue and material to work with.

5 Thank you to my colleagues at DOE for co-hosting
6 this. I thought this was a very productive session and I
7 very much look forward to following-up. Thank you David for
8 ensuring that we stayed within the bounds of our ex parte
9 rules and to the Commission staff and EMR and OER and most
10 especially at OI's for helping pull this together.

11 With that Joe, I will kick it over to you for
12 some final housekeeping items.

13 MR. MCCLELLAND: So, the final housekeeping item
14 is that the Commission will be accepting written
15 post-technical comments to the proceeding. The Docket
16 Number to submit these comments on is AD19-12-000.

17 And with that and with your permission Mr.
18 Chairman, we will adjourn.

19 (Whereupon the Conference adjourned at 3:54 p.m.)
20
21
22
23
24
25

1 CERTIFICATE OF OFFICIAL REPORTER

2

3 This is to certify that the attached proceeding

4 before the FEDERAL ENERGY REGULATORY COMMISSION in the

5 Matter of:

6 Name of Proceeding:

7 FERC/DOE Security Investments for

8 Energy Infrastructure

9

10

11

12

13

14

15

16

17 Docket No.: AD19-12-000

18 Place: Washington, DC

19 Date: Thursday, March 28, 2019

20 were held as herein appears, and that this is the original

21 transcript thereof for the file of the Federal Energy

22 Regulatory Commission, and is a full correct transcription

23 of the proceedings.

24 Larry Flowers

25 Official Reporter