AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 115–531

AN EXAMINATION OF BLACKSTART, THE PROCESS FOR RETURNING ENERGY TO THE POWER GRID AFTER A SYSTEM-WIDE BLACKOUT, AND OTHER SYSTEM RESTORATION PLANS IN THE ELECTRIC UTILITY INDUSTRY

HEARING

BEFORE THE

COMMITTEE ON ENERGY AND NATURAL RESOURCES UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

OCTOBER 11, 2018



Printed for the use of the
Committee on Energy and Natural Resources

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
32–537 WASHINGTON : 2020

COMMITTEE ON ENERGY AND NATURAL RESOURCES

LISA MURKOWSKI, Alaska, *Chairman*

JOHN BARRASSO, Wyoming	MARIA CANTWELL, Washington
JAMES E. RISCH, Idaho	RON WYDEN, Oregon
MIKE LEE, Utah	BERNARD SANDERS, Vermont
JEFF FLAKE, Arizona	DEBBIE STABENOW, Michigan
STEVE DAINES, Montana	JOE MANCHIN III, West Virginia
CORY GARDNER, Colorado	MARTIN HEINRICH, New Mexico
LAMAR ALEXANDER, Tennessee	MAZIE K. HIRONO, Hawaii
JOHN HOEVEN, North Dakota	ANGUS S. KING, JR., Maine
BILL CASSIDY, Louisiana	TAMMY DUCKWORTH, Illinois
ROB PORTMAN, Ohio	CATHERINE CORTEZ MASTO, Nevada
SHELLEY MOORE CAPITO, West Virginia	TINA SMITH, Minnesota

BRIAN HUGHES, *Staff Director*
KELLIE DONNELLY, *Deputy Chief Counsel*
ISAAC EDWARDS, *Special Counsel*
JED DEARBORN, *Counsel*
ROBERT IVANAUSKAS, *FERC Detailee*
MARY LOUISE WAGNER, *Democratic Staff Director*
SAM E. FOWLER, *Democratic Chief Counsel*
JOHN RICHARDS, *Democratic General Counsel*
ELISABETH OLSON, *Democratic FERC Detailee*

CONTENTS

OPENING STATEMENTS

	Page
Murkowski, Hon. Lisa, Chairman and a U.S. Senator from Alaska	1
Cantwell, Hon. Maria, Ranking Member and a U.S. Senator from Washington	2

WITNESSES

Ortiz, Dr. David S., Acting Director, Office of Electric Reliability, Federal Energy Regulatory Commission	4
Ott, Andrew L., President & CEO, PJM Interconnection, L.L.C.	11
Torres, Juan, Associate Laboratory Director for Energy Systems Integration, National Renewable Energy Laboratory	27
Ditto, Joy, President and CEO, Utilities Technology Council	36
Galloway, Sr., Thomas J., President and CEO, North American Transmission Forum	73
Yardley, Timothy M., Senior Associate Director of Technology and Workforce Development, Information Trust Institute, University of Illinois at Urbana-Champaign	97

ALPHABETICAL LISTING AND APPENDIX MATERIAL SUBMITTED

Cantwell, Hon. Maria:	
Opening Statement	2
Diesel Technology Forum:	
Statement for the Record	147
Ditto, Joy:	
Opening Statement	36
Written Testimony	38
Response to Question from Senator Hoeven	114
Galloway, Sr., Thomas J.:	
Opening Statement	73
Written Testimony	75
Responses to Questions for the Record	138
Grid Assurance, LLC:	
Statement for the Record	149
Murkowski, Hon. Lisa:	
Opening Statement	1
Ortiz, Dr. David S.:	
Opening Statement	4
Written Testimony	6
Responses to Questions for the Record	131
Ott, Andrew L.:	
Opening Statement	11
Written Testimony	13
Responses to Questions for the Record	133
Torres, Juan:	
Opening Statement	27
Written Testimony	29
Responses to Questions for the Record	135
Yardley, Timothy M.:	
Opening Statement	97
Written Testimony	99
Responses to Questions for the Record	141

AN EXAMINATION OF BLACKSTART, THE PROCESS FOR RETURNING ENERGY TO THE POWER GRID AFTER A SYSTEM-WIDE BLACKOUT, AND OTHER SYSTEM RESTORATION PLANS IN THE ELECTRIC UTILITY INDUSTRY

THURSDAY, OCTOBER 11, 2018

U.S. SENATE,
COMMITTEE ON ENERGY AND NATURAL RESOURCES,
Washington, DC.

The Committee met, pursuant to notice, at 10:06 a.m. in Room SD–366, Dirksen Senate Office Building, Hon. Lisa Murkowski, Chairman of the Committee, presiding.

OPENING STATEMENT OF HON. LISA MURKOWSKI, U.S. SENATOR FROM ALASKA

The CHAIRMAN. Good morning, the Committee will come to order.

We are here this morning to have a discussion on blackstart, which is the process for returning energy to the power grid after a system-wide blackout.

You do not want to imagine it, but there are probably enough movies that are out there that we do not need to imagine anymore. But just imagine a scenario where everyone living within an interconnected electrical grid system loses power. Here on the East Coast, that would effectively mean a blackout that spans from Maine to Florida, all the way to Minnesota, back to Louisiana. Hundreds of millions of people could be left in the dark, power lines no longer energized, and generating stations would be off.

More practically, it means that your lights would be off, but also your air conditioning is out, kind of a miserable, ugly morning out there and you are going to notice something like that. Appliances like your oven, your refrigerator, your ability to charge your cell phone, no longer working.

A system-wide blackout is mostly the stuff of nightmares and Hollywood thrillers, but it is also a high-consequence threat that our nation must be prepared to respond to. The United States has never seen a blackout of this kind, that I have described of this scope and that is very fortunate, but the increasing risks presented by cyberattacks and the threats of electromagnetic pulse and solar storms make it more important that we be prepared.

The question we have to be able to answer is, should all of the grid go down, how will we restart our generating stations, repower

the lines, and safely deliver electricity to homes and businesses? The process for returning energy to the power grid after a system-wide blackout is known as blackstart. The nuts and bolts of this process are and should be closely held, but we certainly can discuss the theory and the necessity of blackstart in an open setting as we are doing here this morning.

America cannot operate without electricity service, and we must have plans in place to restore power to our grid. A system-wide blackout is a low probability event, but similar to a cyber or nuclear attack, the electric utility industry has to be prepared. There are a variety of everyday threats to the grid that could cause it, like what happened on August 14th in 2003 when we saw a tree that had grown too near a power line and it started this "cascading" blackout, which caused widespread power outages for some 50 million people across the Midwest, the Northeast, and the Canadian province of Ontario.

A cascading blackout occurs when the failure of one interconnected part of the system triggers the failure of successive parts, the domino effect of power transmission failure. Thankfully, the cascading event in August of '03 did not involve the entire interconnection and force us to engage in a real-world test of blackstart procedures, but it could.

I certainly hope our nation never faces a situation where a total restart of the electric system is required, but it is critical and I think we would acknowledge that there has to be a plan in place should the worst happen.

The panel that we have this morning, an impressive group of experts, have all spent time thinking about this, working on these issues. I thank you for making yourselves available this morning. We had to reschedule this hearing from an earlier time, so I appreciate your flexibility. Again, thank you for being here to have this important discussion.

With that, I turn to my colleague, Senator Cantwell.

STATEMENT OF HON. MARIA CANTWELL,
U.S. SENATOR FROM WASHINGTON

Senator CANTWELL. Thank you, Madam Chair. Thanks for scheduling this important hearing and talking about these important issues of preparation and ability to restore our electric grid in the case of a catastrophic system disruption or widespread blackout.

I would also like to commend you, in general, for your continued leadership in this changing energy space. I appreciate the attention the Committee has given to recent hearings, including today's topic of moving forward on reliability.

This is such an important topic because we take for granted that the lights always come on when we flip the switch, but our electric system is increasingly being tested and stressed and there are daily cyber threats to our electricity infrastructure.

In July, the DNI Director spoke to the increase in malicious cyber activities, importantly noting, "the warning lights are blinking red." So I continue to be concerned that there are sophisticated attacks that may result in widespread blackouts.

Unfortunately, cyber threats are not the only concern for the grid. Climate change is resulting in an increased frequency and se-

verity of extreme storm events and natural disasters. With Hurricane Florence hitting the Carolinas, we saw nearly one million customers in the storm path lose power, and widespread flooding that has not yet fully subsided. As we speak, Florida is weathering Hurricane Michael. And, of course, a year ago, the devastation from Hurricane Maria in Puerto Rico still has the island lacking the transmission resiliency in distribution that we would like to see.

On a positive note, I know that the CEO of the North American Electric Reliability Corporation, NERC, has reiterated that it is very unlikely that we would see a foreign entity attack our system, resulting in a catastrophic outage. We know that NERC, FERC and DOE are all working together with our national labs on electricity reliability and continue to move forward on innovative fronts.

But R&D cannot eliminate all the risks. Technologies sometimes fail and, obviously, Mother Nature doesn't always play nice. We must be prepared for major blackout events, and that brings us to this rarely discussed but important topic today, blackstart.

As Congress and regulators of the electricity sector look at grid resiliency, we should consider what we actually have to do to have restoration plans. At the heart of these recovery and restoration plans are generation resources which provide blackstart capability—the ability to restart without drawing on the power grid, which is how generators usually start. Instead, generating units with blackstart capability have the same onsite ability to kick-start the grid. It is important that grid operators and blackstart generators have access to uninterrupted communication as they bring the system back online in a coordinated manner.

I am also encouraged by the innovation in this area of system restoration from blackstart generators. In 2018, the NERC and FERC regional entity joint review of restoration recovery plans found that across all regions of the country, despite an evolving mix of utilities, there is significant reliance on the bulk power system, but they have sufficient blackstart capabilities for their system restoration plans. So that is good. This shows that the changing system can still be resilient.

As an example from last year, Imperial Irrigation District in California successfully demonstrated the use of battery storage energy to fire up a combined-cycle gas turbine from an idle start. And in Pullman, Washington, where we are so proud of Schweitzer Engineering, they tout an island blackstart as a key offering of their comprehensive microgrid system. So I love that; it is so important.

To our friends in the White House and DOE who are continually arguing that only a coal-based system is secure, I would offer two facts: one, without blackstart capability, onsite fuel will not matter when a system is down; and two, clean energy resources can provide resilience, including blackstart, capability. I would point to my home State of Washington, which is blessed with abundant hydropower. The second installment of the Quadrennial Energy Review found that, "hydropower provides a variety of essential reliability services that are beneficial to the electricity system, including blackstart capability."

So again, thank you, Madam Chair, for having this hearing. I appreciate the expert panel that is before us and look forward to

hearing their comments on how we continue to move forward on this innovation and security for our nation.

The CHAIRMAN. Thank you, Senator Cantwell.

We will now turn to our panel. Again, welcome to each of you.

The panel this morning will be led off by Dr. David Ortiz. Dr. Ortiz is the Acting Director for the Office of Electric Reliability over at the Federal Energy Regulatory Commission (FERC). We welcome you this morning.

Mr. Andrew Ott is with us. He is the President and CEO for PJM Interconnection. Thank you for joining us.

Mr. Juan Torres is the Associate Laboratory Director for Energy Systems Integration at NREL, our National Renewable Energy Laboratory. I know that Senator Gardner certainly has an interest in NREL. We are pleased to have you with us, Mr. Torres.

Ms. Joy Ditto is the President and CEO of the Utilities Technology Council (UTC). Welcome.

Mr. Thomas Galloway is the President and CEO for the North American Transmission Forum (NATF). We thank you.

And the panel will be rounded off by Mr. Timothy Yardley, who is the Senior Associate Director of Technology and Workforce Development at the University of Illinois at Urbana-Champaign.

We have a great panel here this morning and are pleased to hear your contribution to this important subject.

Mr. Ortiz, if you would like to lead off. We ask that you try to limit your comments to about five minutes. Your full statements will be incorporated as part of the record.

STATEMENT OF DR. DAVID S. ORTIZ, ACTING DIRECTOR, OFFICE OF ELECTRIC RELIABILITY, FEDERAL ENERGY REGULATORY COMMISSION

Dr. ORTIZ. Thank you, Madam Chairman.

Chairman Murkowski, Ranking Member Cantwell, members of the Committee, thank you for the opportunity to testify today.

My name is David Ortiz. I am the Acting Director of the Office of Electric Reliability at the Federal Energy Regulatory Commission. I'm here today as a Commission staff witness and my remarks do not necessarily reflect those—do not necessarily reflect the views of the Commission nor any individual commissioner.

Congress gave the Commission the authority in the Energy Policy Act of 2005 to oversee the development and enforcement of mandatory reliability standards for the bulk power system. The authority pertains to the interconnected electric reliability, electric system in the United States and excludes Alaska, Hawaii, and local distribution systems.

Section 215 of the Federal Power Act requires FERC to designate an electric reliability organization to develop, with industry, standards to ensure reliable operation of the grid which it proposes to the Commission for approval. NERC is the Commission-certified electric reliability organization.

The subject of today's hearing is blackstart, which is the process of restarting the grid after a blackout. When there is a widespread outage and offsite power is not available, resources that are capable of starting without a connection to the grid are called on to start the process of restoring the grid. These resources are called

blackstart resources and are typically small diesel generators or gas-fired generating units which can be started without power from the grid. Larger hydroelectric units can also be used for blackstart because they require very little initial power to start and can provide a large amount of power quickly.

Reliability standard EOP–005 Version 2, aptly titled "System Restoration from Blackstart Resources," requires responsible entities to have a system restoration plan which includes identifying specific blackstart units to verify the effectiveness of the restoration plan through testing, simulation and analysis of actual events, to keep the restoration plan up-to-date, and to ensure up-to-date system restoration training for operating personnel.

Beginning in September 2014, Commission staff has been collaborating with NERC, the regional entities, utilities and grid operators on a series of studies and reports regarding restoring the grid after a widespread blackout.

In May 2018, staff released the FERC-NERC-Regional Entity Joint Review of blackstart resource availability. The joint team is grateful for the participation of nine anonymous utilities from across the United States for their participation in this study. The study concluded that although some participants have experienced a decrease in the availability of blackstart resources due to the retirement of blackstart capable units over the past decade, the participants have verified that they currently have sufficient blackstart units and resources in their system restoration plans, as well as comprehensive strategies for mitigating against the loss of any additional blackstart resources going forward.

The study recommended that utilities perform expanded testing of the blackstart process when feasible. Doing this requires a utility to take advantage of maintenance outages and other events to test certain aspects of the restoration plan so that real world experiences can supplement the computer simulations that assist in developing such plans. Additionally, the study recommended that utilities assess whether they rely on a single fuel for blackstart and mitigate their reliance on it, if feasible. Further detail is available in my submitted testimony and in the joint study.

I thank the Committee for the opportunity to participate in this hearing and look forward to hearing from the other witnesses and answering your questions.

[The prepared statement of Dr. Ortiz follows:]

Testimony of David S. Ortiz, Ph.D.

Acting Director, Office of Electric Reliability, Federal Energy Regulatory Commission

Before the Committee on Energy and Natural Resources

United States Senate

October 11, 2018

Introduction

Chairman Murkowski, Ranking Member Cantwell, and Members of the Committee, thank you for the opportunity to testify today. My name is David Ortiz. I am the Acting Director of the Office of Electric Reliability (OER) of the Federal Energy Regulatory Commission (FERC or Commission). I am here today as a Commission staff witness and my remarks do not necessarily represent the views of the Commission or any individual Commissioner.

Today, my testimony will provide a brief overview of the Commission's activities to implement its authorities over reliability. Then I will summarize recent work carried out by OER in collaboration with the North American Electric Reliability Corporation and its Regional Entities that assessed how utilities develop and test plans to restore the grid after a blackout, focusing on blackstart.

FERC's Authority to Oversee Reliability

In the Energy Policy Act of 2005, Congress gave the Commission the authority to oversee the development and enforcement of mandatory reliability standards for the Bulk-Power System. The authority pertains to the interconnected electricity system (the "grid") in the United States, and excludes Alaska, Hawaii, and local distribution systems.

Section 215 of the Federal Power Act requires FERC to designate an Electric Reliability Organization (ERO) to develop, with industry, standards to ensure reliable operation of the grid, which it proposes to the Commission for approval. NERC is the Commission-certified ERO. After review and approval by the Commission, compliance with the reliability standards is mandatory by users, owners and operators of the grid in the United States. NERC and its seven Regional Entities enforce the standards and may impose penalties for noncompliance, after notice and opportunity for hearing, subject to review and approval by the Commission. The Commission may also enforce reliability standards independently of NERC.

Importantly, the ERO is responsible for developing and proposing new or modified reliability standards to the Commission. The Commission may approve new or modified reliability standards if it finds them to be "just, reasonable, not unduly discriminatory or preferential, and in the public interest." If a proposed standard does not meet this test, then the Commission may remand it to the ERO for revision. The Commission may not write or modify a reliability standard. If the Commission determines that there is a need for a new or modified standard, it may, on its own motion or upon compliant, direct the ERO to develop and submit a standard to meet the identified reliability need.

Blackstart is the Process of Restarting the Grid after a Blackout

When there is a widespread outage, and offsite power is not available, resources that are capable of starting without a connection to the grid are called on to start the process of restoring the grid. These resources are called "blackstart" resources.[1]

The Emergency Preparedness and Operations, or EOP, reliability standards, seek to ensure that utilities appropriately prepare for extreme events, and blackstart resources and planning are covered in reliability standard EOP-005-2 (System Restoration from Blackstart Resources). The purpose of that standard is to:

> Ensure plans, Facilities, and personnel are prepared to enable System restoration from Blackstart Resources to assure reliability is maintained during restoration and priority is placed on restoring the Interconnection.[2]

Reliability Standard EOP-005-2 contains eighteen requirements to ensure adequate planning, coordination and testing of blackstart. Among others, the standard requires responsible entities: to have a system restoration plan, which includes identifying specific blackstart units; to verify the effectiveness of the restoration plan, through testing, simulation, and analysis of actual events; to keep the restoration plan up-to-date; and to ensure up-to-date system restoration training for operating personnel.

Blackstart capability is important because widespread outages or blackouts can occur resulting in the unavailability of off-site power from the grid. Restoration begins with blackstart units starting. These units energize a particular set of transmission lines and serve certain loads, with the goal of providing offsite power to larger generating units that can serve more load. The series of lines that are energized as part of a blackstart plan are called "cranking paths."

Blackstart units are typically small diesel generators or gas fired generating units which can be started without power from the grid. Larger hydroelectric units can also be used for blackstart because they require very little initial power to start, and can provide a large amount of power quickly. Staff's recent review of entities' blackstart plans showed that a utility in Southern California successfully demonstrated the use of a battery energy storage system to provide blackstart service. In addition to these blackstart units identified in entities' blackstart plans, entities also have access to other blackstart-capable units.

---

[1] NERC defines a blackstart resource as a "generating unit(s) and its associated set of equipment which has the ability to be started without support from the Bulk Electric System or is designed to remain energized without connection to the remainder of the System, with the ability to energize a bus, meeting the Transmission Operator's restoration plan needs for Real and Reactive Power capability, frequency and voltage control, and that has been included in the Transmission Operator's restoration plan." *See* NERC Glossary of Terms, https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf.

[2] https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=EOP-005-2&title=System%20Restoration%20from%20Blackstart%20Resources&jurisdiction=United%20States

The FERC-NERC-Regional Entity Review of Blackstart Resource Availability and Testing

Beginning in September 2014, Commission staff has been collaborating with NERC, Regional Entities, utilities and grid operators on a series of studies and reports regarding restoring the grid after a widespread blackout. The motivation for the initial study was to get a comprehensive understanding of the electric utility industry's bulk-power system recovery and restoration planning, focusing specifically on the reliability standards relevant to system recovery and restoration, which require entities to develop and test plans for recovery and restoration. To do this, Commission staff worked collaboratively with staff from NERC and the Regional Entities to review the plans for recovery and restoration of utilities of participating utilities. Utilities participated voluntarily in the joint reviews, which identified and documented best practices, and were not compliance audits or enforcement investigations. Since the release of the initial study in January 2016, the joint study team has released two additional studies. The latest study, focused on blackstart, is the main topic of this hearing.

In May 2018, staff released the *FERC-NERC-Regional Entity Joint Review of Blackstart Resources Availability (BRAv).* This study took a close look at: "(1) the availability of blackstart resources, including the identification of strategies for replacing these resources going forward and the factors to be considered for such replacement resources; and (2) options for expanding system restoration plan testing beyond the currently required blackstart resource testing, to ensure that a blackstart resource can energize equipment necessary to restore the system as intended in the restoration plan."[3] The study also included an assessment of registered entities' blackstart resource testing under anticipated blackstart conditions to ensure that these resources can effectively restore the bulk-power system following a widespread outage.

The joint team is grateful for the participation of nine anonymous utilities for their participation in the study. Staff considered the following factors when identifying participants: those with significant grid operational responsibilities; utilities in different regions so as to document regional differences; those that have or are experiencing changes in their blackstart resources; those that have conducted expanded testing of blackstart; those that have experience with large-scale system restoration.

Based on staff's observations of the participating utilities, the overwhelming majority of blackstart units are gas turbines, diesel generators, and pumped and traditional hydroelectric facilities. During staff's recent review of entities' blackstart plans, several participants indicated that the total number of available blackstart-capable units in their respective footprints has decreased over time due to the impact of regulations and the retirement of non-economic or aging assets.

The study concluded that although some participants have experienced a decrease in the availability of blackstart resources due to retirement of blackstart-capable units over the past decade, the participants have verified they currently have sufficient blackstart resources in their system restoration plans, as well as comprehensive strategies for mitigating against loss of any

[3] *FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans: Blackstart Resource Availability*, at 1.

additional blackstart resources going forward. The study also found that participants that have performed expanded testing of blackstart capability, including testing energization of the next-start generating unit, gained valuable knowledge that was used to modify, update and improve their system restoration plans. Participants also used the knowledge gained to update and improve their existing steady state and dynamic models of those plans, as well as their system restoration drills.

The study recommended that utilities perform expanded testing of blackstart cranking paths where feasible. Doing this requires a utility to take advantage of maintenance outages and other events to test certain aspects of the restoration plan so that real-world experiences can supplement the computer simulations that assist in developing such plans. Additionally, the study recommended that utilities assess whether they rely on a single fuel for blackstart and mitigate their reliance on it if feasible. Further the report recommended that utilities verify the accuracy of simulations of their blackstart plans to ensure these plans would work during actual system restoration. For those utilities that reported a decline in the number of available blackstart units, the entities reviewed have verified that they have sufficient blackstart resources to support their current restoration plans. The study recommended that, if relevant, the utility examine the adequacy of their compensation for blackstart services, potentially including next-start generators and participation in expanded testing.

Ensuring reliable operations of the grid relies on real-time monitoring and control of thousands of transmission system components scattered across a wide area. To support these operations, utilities rely on both proprietary and contracted communications systems, supervisory control and data acquisition (SCADA) systems, and energy management systems (EMS). Utilities have made significant investments in these systems and seek for them to be as redundant and available as possible.

In the event of a widespread blackout, however, there is a concern that the sensors and computer systems that utilities use to operate the grid would be unavailable to support restoration. Substations include backup battery power to support these systems for a short time, but they could become depleted and unable to support restoration. To investigate whether utilities were adequately prepared for such a situation, Commission staff, along with NERC and the Regional Entities conducted a joint study that evaluated the ability of utilities to restore the grid in the absence of remote grid measurements, communications, and software support systems. Similar to the study regarding blackstart discussed earlier, the joint study team worked with eight volunteer utilities to evaluate their ability to carry out their restoration plans in the absence of EMS or SCADA.

The joint study on Planning and Restoration absent EMS or SCADA (PRASE) showed that without these systems the study participants would remain capable of executing their restoration plans. Some of the participants specifically planned for system restoration without EMS or SCADA. Other participants emphasized emergency preparedness for challenging restoration conditions without specifically planning for the loss of EMS or SCADA. The participants acknowledged, however, that complete restoration would be more time consuming and labor intensive without their computer support systems. In particular, the steps of the restoration

process that require wider coordination, and those steps performed during later stages of the restoration process, include load pick up, managing voltage and frequency, and synchronization with other islands or systems. To restore the grid without access to EMS and SCADA, the joint study team found that participants would use support engineers to aid the transmission system operators in the analyses needed for system restoration. For example, additional operations engineering support and power system modeling staff using offline power flow tools would simulate restoration steps to assist operators in their decision-making process. Additionally, the restoration team would manually record the status of the grid during the restoration process. Manual restoration of the grid would require utilities to deploy personnel to the field, and would require robust backup communications systems.

The joint study team recommended that utilities prepare for this situation by assessing the availability of backup power, the adequacy communications, and personnel requirements. Further, the joint study team recommended that utilities include restoration without EMS or SCADA in their restoration exercises.

I thank the Committee for the opportunity to participate in this hearing and look forward to answering your questions.

The CHAIRMAN. Thank you, Dr. Ortiz.
Mr. Ott.

STATEMENT OF ANDREW L. OTT, PRESIDENT & CEO, PJM INTERCONNECTION, L.L.C.

Mr. OTT. Chairman Murkowski, Ranking Member Cantwell and members of the Committee, thank you so much for having me back again. I was here in January talking about cold weather operations, and I'm really honored to be here today to talk about the important topic of blackstart.

But before I begin, I would like to acknowledge the hard work of our utility partners in Florida, the Carolinas, and Northern, excuse me, Southern Virginia, to restore power in the aftermath of the hurricanes, not only the current one, Michael, but Florence just a few weeks ago. Again, the power industry has been the model of cooperation and collaboration and, frankly, they have all of our appreciation for the types of good work they do.

PJM operates the largest power grid in the nation. We serve almost a quarter of the electricity consumed within the United States, population of 65 million people, 13 states and the District of Columbia. Our role is three-fold: we essentially ensure the operation and reliability of the bulk power grid; we operate the competitive wholesale markets; we also coordinate regional planning for the future evolution of the grid.

I want to underscore today for you a couple key points related to the topic of blackstart. First, reliability and effective restoration of service are key and top priorities for organizations like PJM and utilities. We work with our members as well as state and local governments. We take this task very seriously. We plan, we drill, and the location of blackstart resources is well known in advance. We also work with, of course, the federal regulator and FERC and NERC. The second is, restoration of service is a shared responsibility. The local utility, organizations like PJM which are regional transmission organizations, of course end-use customers themselves, federal and local and state authorities.

Three key parts to this responsibility. One is restoration of critical resources, known as blackstart resources. So those blackstart resources are contracted by us in advance to provide such services. I do want to clear up some misconceptions about blackstart resources. Coal and nuclear generators are generally not blackstart. Blackstart resources tend to be more flexible, smaller units like gas units or, as Ranking Member Cantwell indicated, hydro resources. The priority restoration of facilities, end-use facilities, those that would be restored first, is also something we do in advance to look at how do we, what's the plan, if you will, once we re-enable the grid with blackstart resources to bring back customers in an orderly manner. And the last is, of course, coordination of individual customer backup generation and how they integrate into the grid.

Our role as an RTO, again, is one of coordination and, in these types of events, we coordinate the start of reenergizing the system and work with all parties, including utilities. The utilities, of course, and state and local government agencies, again, are critical to this restoration effort because they have the physical energization of the grid.

A couple things about the system. We get that the risks are changing. What—as you mentioned, cyberattacks, potential sabotage, other types of things that we really didn't dream of some years ago. From our perspective at PJM, the way we look at that, one of our main control systems, the EMS system, we actually have a copy of that. We have more than one copy, of course, we probably have four or five different—and one of them is air-gapped. It sits in a dark room. Should our systems become compromised by a cyberattack, we can jettison that whole system, bring up a fresh one and reconnect within a very quick, I can't say what it is, but a very quick time.

One effort, too, is resilience for the grid. We look at how—what are the dependencies? PJM is essentially looking at, if you will, as resilience, the dependency—people have a legitimate question as we get more and more dependent upon natural gas resources, you'll see retirement of coal and nuclear.

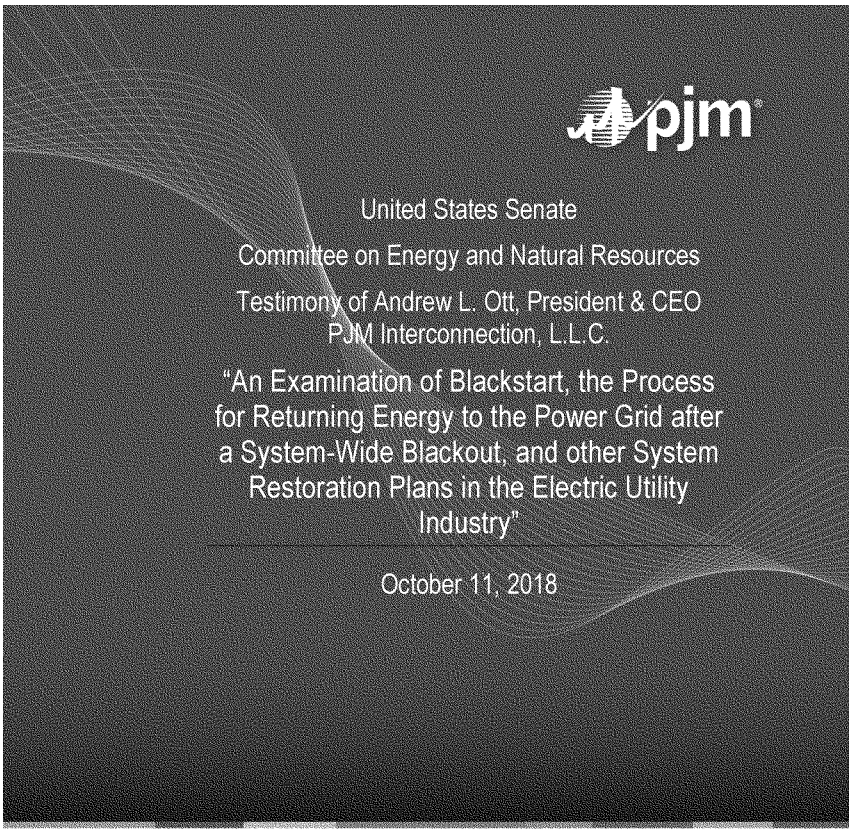
The question is being asked, are we vulnerable? And I think it's an absolutely legitimate question. We're taking that on. On November 1st, PJM will issue a fuel security study, looking out into 2023 to say, are we vulnerable? What are the pinch points? It's an analytical approach, and we will be, obviously, sharing that information with, not only yourselves, but others.

One thing, role, you could play, as I look at things we need, as we look at resilience in these types of paying resources for the characteristics and attributes they provide. We've put in quite a few suggestions to FERC. Realizing they're a busy organization, we really need to move forward with some of these issues about paying resources for their reserve characteristics, paying resources for their fuel security characteristics. We really need to move on with that.

I really thank you for your attention today, and I am ready for questions once we're through the initial dialogue.

Thank you very much.

[The prepared statement of Mr. Ott follows:]

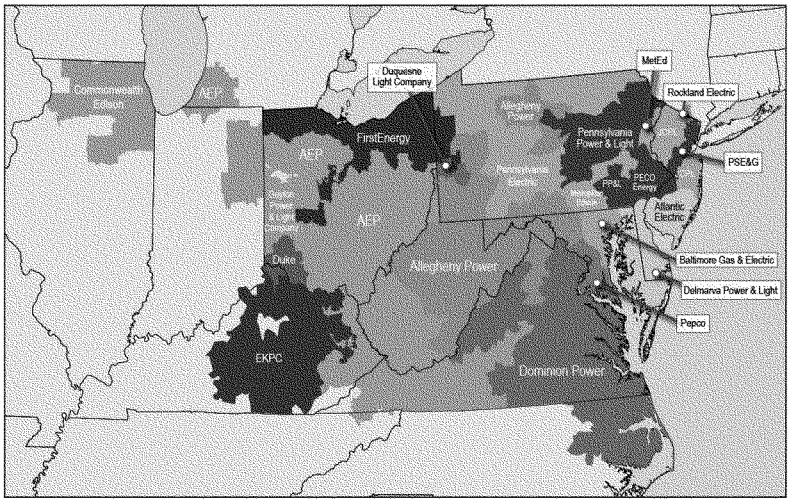


Testimony of Andrew L. Ott

President & CEO
PJM Interconnection
October 11, 2018

Andrew L. Ott
President & CEO
PJM Interconnection

Thank you for the opportunity to testify today. I am Andrew Ott and serve as President and CEO of PJM Interconnection. PJM is the regional transmission organization responsible for the reliable operation of the bulk electric power grid serving 65 million people in all or parts of Delaware, Illinois, Indiana, Kentucky, Maryland, Michigan, New Jersey, North Carolina, Ohio, Pennsylvania, Tennessee, Virginia, West Virginia and the District of Columbia. PJM operates the largest bulk power system in the nation, and serves almost a quarter of the country's electricity needs.



Before I begin today, I want to acknowledge the hard work of the staff of Dominion Energy and Duke Energy, two PJM members, as they worked to restore power lost as a result of Hurricane Florence in North Carolina.

The eastern shore of North Carolina is in the PJM service territory. While this effort was primarily led by the local utilities, we coordinated closely with these affected PJM members and appreciate all of the effort by the industry as a whole to continue to make sure reliability and prompt service restoration are the first priority.

I. Introduction and Overview

I want to lead off today with some key points for your consideration:

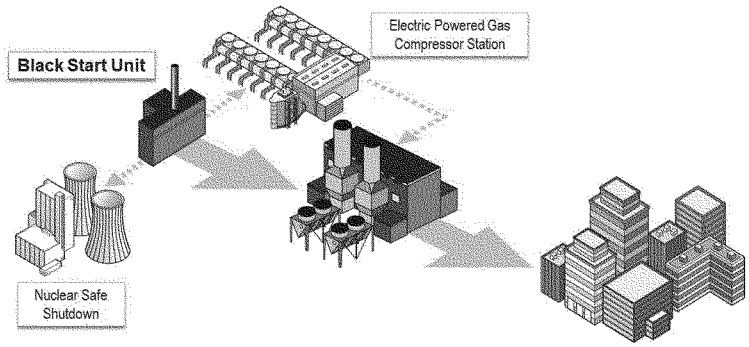
- **Reliability and Effective Restoration of Service Are the Top Priorities for a Grid Operator**: Restoration of service in response to natural disasters as well as potential physical or cyberattacks is not a new task for PJM or any other system operator. We have established processes and procedures in place, and working with the individual utilities in our region as well as with our neighbors, we drill for these events continuously.

Restoration is a key part of our reliability responsibilities at PJM and is something we take extremely seriously.

- **Restoration of Service Is a Shared Responsibility:** Restoration of service is a shared responsibility among local utilities, regional transmission organizations (RTOs) such as PJM, and end-use customers, as well as the federal government and state and local authorities.

  There are three key aspects of the important task of recovering from a disruption and restoring service to customers, including special roles assigned to the federal government and the states:

  1. **Restoration of Critical Loads:** One of PJM's key roles is to ensure service to key strategically located generators, known as black start resources, which can start without needing to draw power from the grid. These quick-start resources are then utilized to energize transmission lines and restart other generators, which in turn are needed to restart other generators needed to restore the grid and ultimately get customers back online. The black start resources also provide safe shutdown power for nuclear units and ensure service to critical natural gas facilities needed to fuel larger generators during the restoration process. We refer to this as restoration of critical loads.



  2. **Priority Restoration to Key End-Use Facilities:** Local utilities and the states play key roles in prioritizing restorations at the distribution level to hospitals, National Guard facilities, critical communication equipment and other locations critical to public health and safety. The specific priorities and plan for each utility are often described in tariffs and regulations adopted and overseen by state public utility commissions.

  3. **Individual Customer Backup Generation:** In addition to these systemwide efforts, a number of end-use customers, including Department of Defense facilities and others, also invest in their own backup generation. This is often referred to as "behind-the-meter" generation. PJM is working on improving visibility of and communication to these behind-the-meter resources in order to take them into account in our own restoration plans and, with the customer's consent, to be able to dispatch any excess capacity from these resources to meet the needs of others. We refer to this as enhancing the visibility and dispatchability of these individual customer resources and it is a combined effort with key end-use facilities in our region such as military bases.

- **Restoration of Systems from a Cybersecurity Event Requires Enhanced Coordination and Redundancy:** Threats like electromagnetic pulses and cyberattacks require us to look at restoration

differently than severe weather, given their ability to impede traditional restoration activities by targeting the tools and systems we use to operate and restore the grid. While a cyberattack could cause an outage requiring black start, the presence of an active adversary and the extent of a cyber intrusion can affect the availability of the industrial control system (ICS) and supervisory control and data acquisition (SCADA) tools the industry uses to remotely execute black start and other vital grid functions. Therefore, industry and government continue to evolve to consider new threats that may require more advanced methods to restore the system following an outage that also account for communications and data disruptions stemming from a targeted attack. This includes work on redundant communications systems, joint training between industry and government cyber-response capabilities and updates to black start plans to add operational flexibility.

All of the above aspects of recovering from a disruption and restoring service are important considerations for the reliable provision of electricity, and supporting interdependent critical services, and are the focal points of PJM's near-term resilience activities. All of these efforts work together to ensure timely service restoration.

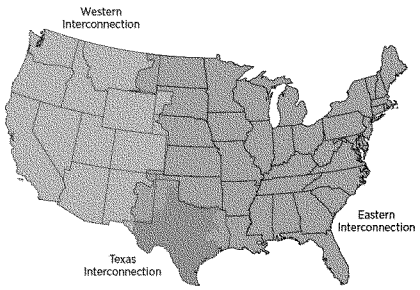
Action Steps Going Forward

Ensuring a Resilient Grid: PJM is working to ensure that the grid, which is reliable today, is also resilient when faced with new levels of cyber and physical threats. This too is a responsibility that is shared, with key roles for the Federal Energy Regulatory Commission (FERC), the Department of Energy, the Department of Homeland Security, PJM, our member companies, and state and local public officials. The grid is reliable today and will continue to be into the future. The goal of our resilience efforts is to ensure that the grid can withstand prolonged outages from events that pose risks beyond what is covered by today's reliability standards.

Encouraging Interagency Coordination: It remains critical that the various agencies of the federal government approach this issue in an organized, cohesive fashion. Although much coordination occurs today among FERC, the Department of Energy and the Department of Homeland Security, additional work is needed and appropriate to bring in and harmonize the work of other key agencies. These include the Transportation Security Administration, which is responsible for overseeing the physical security and cybersecurity of the gas pipeline system, and the Federal Communications Commission, which plays a critical role in allocating spectrum to enable key communications in the event of an extended outage. This effort requires intergovernmental coordination and was a recommendation we highlighted prominently in our comments to FERC in our reply to the Docket No. AD18-7-000, "Grid Resilience in Regional Transmission Organizations and Independent System Operators." I have included the executive summary of our recommendations to FERC of specific resilience action steps it could take in the attachment to my testimony.

II. Defining Terms

The term "black start" is often misunderstood. Since the Eastern, Western and Texas Interconnections are, in essence, three large synchronous machines, a system outage caused by a downed transmission line or voltage collapse on one part of the grid can often be isolated through the use of relays and circuit breakers. In such instances, system restoration is accomplished by carefully resynchronizing the isolated grid to the rest of the grid.



Restoration of the grid from a black start condition occurs when an entire interconnection (Eastern, Western or Texas) is down, and there is no other part of the interconnection that is available to connect in order to synchronize the isolated part of the grid to the rest of the operating grid. In such an instance, we call on black start resources, which are generators

strategically located at key points on the grid that are able to start without the help of electric power in order to start other generators and natural gas compressor stations that are dependent on electric power. As those generators in turn are energized and synchronized to the grid, they restore power to other generators, which results in restoration of service to end-use customers.

Although we procure black start resources and test them regularly, I am pleased to report that PJM has never had to call upon these resources to operate in a restoration event. This is because we have not, to date, experienced an interconnection-wide outage that has prevented us from "jump-starting" one part of the grid by synchronizing it with another part. Nevertheless, the service is critically important, and procuring sufficient black start resources is a responsibility we take seriously.

III. The Impact of Retirements of Nuclear and Coal Resources

Discussion around ensuring adequate black start resources is a different discussion from the important focus we have had on recent announced retirements of nuclear and coal resources. Black start units are, by definition, small, quick-start resources that can energize very quickly and otherwise may operate quite infrequently. For this reason, natural gas combustion turbines are currently the technology of choice for black start, although strategically placed batteries are an emerging promising black start technology. As to the interaction of nuclear units to black start units, we use black start resources to ensure the safe shutdown of nuclear facilities — not to re-energize those resources back onto the grid after a shutdown. Synchronizing a nuclear unit back onto the grid after a loss of part or all of the grid is a more complex process that requires potential Nuclear Regulatory Commission review and a time for the unit to ramp back to full production levels.

IV. Looking Forward: The Role of Resilience Planning as It Affects System Restoration

Although, as outlined above, black start is a distinct service, PJM's activities to ensure a resilient grid have also taken a larger focus. After the 2014 Polar Vortex, with the support of FERC, we made significant changes to enhance the performance of the generation resources on which we rely. This initiative, known as Capacity Performance, has led to a noticeable improvement in generation fleet performance, as we detailed in our 2018 white paper "Strengthening Reliability: An Analysis of Capacity Performance." As noted in that analysis:

> "During the cold snap of 2017–18, Capacity Performance resources' forced outage rates were significantly lower than during the 2014 Polar Vortex (5.5 percent vs. 12.4 percent). Other indicators of the effectiveness of Capacity Performance include improvements of over 50 percent in many operating parameters after the implementation of Capacity Performance, such as a decrease in restrictive generator operating parameters, reported investment in major reliability work for existing resources, and new resources investing in firm gas and transportation contracts."

In early 2017, we issued a fuel analysis paper, "PJM's Evolving Resource Mix & System Reliability," which concluded that the PJM system can remain reliable with the addition of more natural gas and renewable resources, but that heavy reliance on any one resource type raises questions about electric system resilience beyond existing reliability standards.

We are currently embarking upon a detailed fuel security analysis that builds on our past work by looking beyond reliability to the ability of the grid to withstand extreme events of extended duration. Our analysis will consider the advantages and disadvantages of each fuel type during extended events, recognizing the impact of the increased penetration of natural gas and renewable resources as nuclear and coal generation resources retire.

Although our conclusions will be released shortly, I can observe two key points so far:

- **Resilience Issues Are Location-Specific.** An electric generator sitting virtually on top of shale gas wells is potentially as fuel secure as a coal plant with an adjacent coal pile or a nuclear facility with fuel rods on-site. On the other hand, a natural gas generator without dual fuel and served off of a single lateral natural gas line is clearly not as resilient. As in real estate, "location matters."

- **Policymaking Guidance Is Needed**: As with any exercise of this sort, there is a balance that policymakers will need to strike. We need to ensure the grid is resilient to extreme but plausible events and need to decide the degree of resilience investment that is reasonable for the ratepayers of the region to bear. The ratepayers of our region, be they households or businesses, shouldn't be responsible for securing the grid from a World War III type of attack. At some point, that becomes the task of national defense, paid for by taxpayers across the land. On the other hand, once we issue the results of our analysis, we intend to work with stakeholders to consider how best to value fuel security beyond the initiatives we have already undertaken through our Capacity Performance construct. Nevertheless, PJM cannot do this alone. As noted previously, we proposed 10 specific recommendations to FERC of concrete steps that can be taken to provide that critical guidance. We respectfully await their action on those initiatives and other related issues.

PJM has worked to serve as a resource to this Committee on a host of issues, ranging from questions associated with reliability to the operation of our markets. We pledge to continue to serve in that role as you weigh these important national policy issues.

Thank you again for this opportunity, and I look forward to your questions and comments.

Attachment: Recommendations of Specific Resilience Action Steps from PJM Interconnection Response to FERC Grid Resilience Proceeding

UNITED STATES OF AMERICA BEFORE THE FEDERAL ENERGY REGULATORY COMMISSION

Grid Resilience in Regional Transmission Organizations and Independent System 000 Operators	)))))	**Docket No. AD18-7-**

COMMENTS AND RESPONSES OF PJM INTERCONNECTION, L.L.C.

Craig Glazer
Vice President, Federal Government Policy
PJM Interconnection, L.L.C.
1200 G Street, NW, Suite 600
Washington, DC 20005
(202) 423-4743 (phone)
Craig.Glazer@pjm.com

Jacqulynn Hugee
Associate General Counsel
PJM Interconnection, L.L.C.
2750 Monroe Boulevard
Audubon, PA 19403
(610) 666-8208 (phone)
Jacqulynn.Hugee@pjm.com

Christopher O'Hara
Vice President, Deputy General Counsel
PJM Interconnection, L.L.C.
2750 Monroe Boulevard
Audubon, PA 19403
(610) 666-3433 (phone)
Christopher.OHara@pjm.com

Counsel for PJM Interconnection, L.L.C

March 9, 2018

UNITED STATES OF AMERICA BEFORE THE FEDERAL ENERGY REGULATORY COMMISSION

Grid Resilience in Regional Transmission Organizations and Independent System 000 Operators	)))))	**Docket No. AD18-7-**

COMMENTS AND RESPONSES OF PJM INTERCONNECTION, L.L.C.

PJM Interconnection, L.L.C. ("PJM") hereby submits its comments and responses ("Comments") to the resilience issues and inquiries identified in the Federal Energy Regulatory Commission's ("Commission") Order Terminating Rulemaking Proceeding, Initiating New Proceeding, and Establishing Additional Procedures issued on January 8, 2018.[1] Through these Comments, PJM:

- outlines the considerable steps PJM and its stakeholders have undertaken, or have actively underway, to enhance the resilience of the portion of the Bulk Electric System[2] ("BES") operated by PJM, and

[1] *Grid Resilience in Regional Transmission Organizations and Independent System Operators*, 162 FERC ¶ 61,012 (2018) ("Grid Resilience Order"). In the Grid Resilience Order the Commission (1) terminated the proceeding regarding the proposed rule on Grid Reliability and Resilience Pricing submitted to the Commission by the Secretary of the United States Department of Energy ("DOE") that was focused on providing cost-of-service compensation to generators with on-site fuel capability, and (2) initiated the above-captioned proceeding on Grid Resilience in Regional Transmission Organizations and Independent System Operators. The Grid Resilience Order directed each Regional Transmission Organization ("RTO") and Independent System Operator ("ISO"), including PJM, to submit initial comments and responses to the Commission on resilience in order to enable the Commission to holistically examine the resilience of the bulk power system. Hereinafter, RTOs and ISOs are referred to collectively as RTOs.

[2] In its questions, the Commission referenced the resilience of the bulk power system. In its responses, PJM is addressing resilience as it relates to the Bulk Electric System. The North American Electric Reliability Corporation ("NERC") defines Bulk Power System as: (A) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and (B) electric energy from generation facilities needed to maintain transmission system reliability. The term does not include facilities used in the local distribution of electric energy. NERC defines Bulk Electric System as: "Unless modified by the lists shown below, all Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electric energy…" (the detailed list of systems modifying the definition are not provided herein). *See Glossary of Terms*

- details specific action steps the Commission (in some areas working with other federal and state agencies) could undertake to enhance overall resilience of the BES not just in the PJM Region but potentially across the nation.

Just as with so many issues before the Commission, enhancing grid resilience requires a careful balancing of many competing interests. Ultimately, the goal is to ensure that the BES can continue, into the future, to meet the needs of customers for the reliable and secure delivery of electricity at a price which remains just and reasonable. PJM has approached these Comments by striving to balance those different concerns and interests.

I. INTRODUCTION

There are a number of important initiatives that are underway and others that should be enhanced and made part of the Commission's focus with respect to system resilience. Defining resilience is an important first step as outlined below. Addressing the issues raised in the Commission's inquiries to the RTOs is an important second step.[3]

As a multi-state RTO, PJM has visibility into interstate and inter-system resilience vulnerabilities and restoration challenges. PJM's role in the resilience effort is not an exclusive role, but a partnership role that involves interaction and coordination with member Transmission Owners,[4] Load Serving Entities, end-use customers, the Commission, other federal and state agencies and regulatory commissions, and other stakeholders. But given the interconnected nature of the electric power grid, there is an important federal interest that must be recognized and advanced in addressing resilience. As a result, as proposed herein, the Commission should

---

Used in NERC Reliability Standards, North American Electric Reliability Corporation (Jan. 31, 2018) ("NERC Glossary"), www.nerc.com/files/glossary_of_terms.pdf.

[3] Although PJM is supportive of this docket starting with an inquiry to the RTOs, grid resilience issues are not limited to RTOs. If anything, because of their scale and scope, RTOs are best able to evaluate overall grid resilience issues of the BES in their footprints. But the scope of the Commission's effort should in no way be limited to RTOs since many if not most BES grid resilience issues are truly national in scope.

[4] All capitalized terms that are not otherwise defined herein have the meaning as defined in the PJM Open Access Transmission Tariff ("Tariff"), Amended and Restated Operating Agreement of PJM Interconnection, L.L.C. ("Operating Agreement"), and Reliability Assurance Agreement Among Load Serving Entities in the PJM Region.

advance additional processes that could help with additional coordinated identification, authentication and mitigation of future grid resilience challenges, and authentication and mitigation of the vulnerabilities that currently exist.

To be clear, the PJM BES is safe and reliable today – it has been designed and is operated to meet all applicable reliability standards. However, improvements can and should be made to make the BES more resilient against known and potential vulnerabilities and threats. In many cases, resilience actions are anchored in, but go beyond what is strictly required for compliance with, the existing reliability standards. As a result, PJM has identified a number of recommended initiatives.

II. EXECUTIVE SUMMARY

In its broadest sense, resilience involves preparing for, operating through, and recovering from events that impose operational risk, including but not limited to high-impact, low-frequency events. However, resilience is not only about high-impact, low-frequency events. Rather, resilience also involves addressing vulnerabilities that evolved over time and threaten the safe and reliable operation of the BES (or timely restoration), but are not yet adequately addressed through existing RTO planning processes or market design. Many of the actions, policies, procedures, and market structures designed to improve system resilience are scalable and applicable to a wide range of potential risks and impacts. The challenge lies in the nature of high-impact, low-frequency events, because they are not amenable to quantitative, probability- based analyses commonly used for risk management[5] due to the difficulty of predicting the timing and impact of their occurrence. Probabilities of high-impact, low frequency events are generally unknown or extremely difficult to quantify, and the consequences or impacts of high-

[5] *See e.g.* Kaplan, S. and Garrick, B.J. (1981). On the Quantitative Definition of Risk. *Risk Analysis* 1(1).

impact, low-frequency events - although assumed to be intolerably high in terms of both human and economic costs - are difficult to quantify. Prudent resilience efforts to address verifiable vulnerabilities and threats are worthwhile despite the uncertainty, and can be effectively and efficiently managed through the use of a range of complementary analyses and strategies.

Accordingly, PJM requests that the Commission take the following actions to enhance resilience of the grid and interrelated systems that depend on the BES.

- Finalize through this proceeding a working definition and common understanding of grid resilience, clarifying that resilience resides within the Commission's existing authority with respect to the establishment of just and reasonable rates, terms and conditions of service under the Federal Power Act ("FPA").[6]
- Establish a Commission process, either informally through one or more of the Commission's existing offices, or formally through a filing process, that would allow an RTO to receive verification as to the reasonableness of its assessments of vulnerabilities and threats, including Commission utilization of information that may be available to it, but not available to the RTO because of national security issues. Those assessments, once verified, could then form the basis for RTO actions under its planning or operations authority consistent with its tariffs. Simply put, in coordination with other federal agencies such as the United States Department of Defense ("DOD"), DOE, United States Department of Homeland Security ("DHS"), as well as NERC, the Commission needs to provide intelligence and metrics to apply to resilience vulnerability and threat analyses that can then guide and anchor subsequent RTO planning, market design, and/or operations directives.[7]
- Articulate in this docket that the regional planning responsibilities of RTOs currently mandated under 18 CFR § 35.34(k)(7), and the NERC TPL standards (which among other things require RTOs to plan to provide reliable transmission service and assess Extreme Events to the BES), includes an obligation to assess resilience. The Commission should consider, after confirming that resilience is a component of such planning, initiating appropriate rulemakings or other proceedings to further articulate the RTO role in resilience planning including

[6] *See, e.g.*, Section 215, 16 U.S.C. §824o.

[7] Through this process, PJM would be seeking verification that its vulnerability identification or threat assessment is consistent with information (including classified information not necessarily available to PJM) held by the federal government and thus should be used to guide future actions. The verification would be solely of the identified vulnerability or assessed threat and would not preclude challenges in the context of a rate proceeding or otherwise as to the cost efficiency of addressing the vulnerability or threat.

affirmative obligations and standards to plan, prepare, mitigate, etc. As part of this effort, the Commission should reconcile its continued interest in transparency in planning processes under Order Nos. 890 and 1000 with the challenges of public disclosure of significant grid resilience vulnerabilities. Working with stakeholders, PJM has begun this process to include existing standards like NERC CIP-14 critical facilities and urges the Commission to provide assistance to ensure that the goals of transparency and information to end users do not become a means to disclose grid vulnerabilities that can be exploited by those with bad intent.

- Require that all RTOs (and jurisdictional transmission providers in non-RTO regions) submit a subsequent filing, including any necessary proposed tariff amendments, to implement resilience planning criteria, and develop processes for the identification of vulnerabilities, threat assessment and mitigation, restoration planning, and related process or procedures needed to advance resilience planning.
- Request that all RTOs (and jurisdictional transmission providers in non-RTO regions) submit a subsequent filing, including any necessary proposed tariff amendments, for any proposed market reforms and related compensation mechanisms to address resilience concerns within nine to twelve months from the issuance of a Final Order in this docket. PJM, together with its stakeholders, is already actively evaluating such potential reforms that advance operational characteristics that support reliability and resilience, including (i) improvements to its Operating Reserve market rules and to shortage pricing, (ii) improvements to its Black Start requirements, (iii) improvements to energy price formation that properly values resources based upon their reliability and resilience attributes, and (iv) integration of distributed energy resources ("DERs"), storage, and other emerging technologies. A deadline for submission of market rule reforms that the RTO feels would assist with its resilience efforts would help ensure focus on these issues in the stakeholder process.
- Request that PJM submit a subsequent filing, including any necessary proposed tariff amendments, to permit non-market operations during emergencies, extended periods of degraded operations, or unanticipated restoration scenarios. Such filings could including provisions for cost-based compensation when the markets are not operational or when a wholesale supplier is directed to take certain emergency actions by PJM for which there is not an existing compensation mechanism.[8]
- Establish improved coordination and communication requirements between RTOs and Commission-jurisdictional natural gas pipelines to address resilience as it relates to natural gas-fired generation located in RTO footprints. With respect to interstate pipelines, PJM respectfully requests that the Commission launch

[8] Any such RTO procedures would be limited, and would not interfere with DOE emergency actions under FPA, sections 202(c) or 215A. 16 U.S.C. §§ 824a(c), 824o-1.

additional initiatives addressing the interaction between RTOs and interstate natural gas pipelines as follows:

- PJM supports additional reforms to Order No. 787 to avoid the variable levels of information sharing provided by different pipelines in the PJM Region that resulted from the strictly voluntary nature of Order No. 787.
- PJM requests additional efforts by the Commission to encourage sharing of pipelines' prospective identification of vulnerabilities and threats on their systems and, sharing on a confidential basis in real-time, the pipeline's modeling of such contingencies and communication of recovery plans. This would ensure that the RTO has the best information in real- time to make a determination whether to increase Operating Reserves or take other emergency actions in response to a pipeline break or other contingencies occurring on the pipeline system. Although a degree of effective coordination and communication with the pipelines serving the PJM Region has been achieved, more of a focus on real time coordination of modeling of contingencies and real-time communication of same would ensure greater consistency in coordination and information and can bring gas/electric coordination, to the next level to face the next generation of resilience issues. Accordingly, PJM recommends a more holistic regulatory framework for identifying and coordination of modeling of (1) pipeline contingencies in RTO planning and (2) real-time impacts of adverse pipeline events on BES operations.
- PJM requests an increased focus on restoration planning coordination between RTOs and pipelines as each entity has valuable information that can affect the other's timely restoration.
- PJM urges the Commission to encourage the development of additional pipeline services tailored to the flexibility needs of natural gas-fired generation so as to encourage appropriate tailoring and pricing of services beyond today's traditional firm/interruptible paradigm.
- PJM believes that much can be done both in the Commission's exercise of jurisdiction over RTOs as well as interstate pipelines to improve generation interconnection coordination with pipelines in order to better align interconnection activities and timelines and minimize potential issues associated with generation facilities located in areas on pipeline systems where reliability or resilience benefits may be sub-optimal.
- Finally, PJM believes that more action is needed to support the harmonization of cyber and physical security standards between the electric sector and the natural gas pipeline system. PJM recognizes that this matter spans beyond the Commission but also involves the Transportation Security Administration ("TSA") and Pipeline and Hazardous Materials Safety Administration ("PHMSA"), but believes that through greater inter-agency coordination, a base level of resilience to

physical and cyber-attacks can be achieved even while still respecting the different regulatory authorities of each agency.

- In addition, greater communication and coordination is needed with the local distribution companies ("LDCs") that supply wholesale generation, and the Commission should support such efforts including evaluating whether communication and coordination obligations should be imposed on LDCs that supply jurisdictional wholesale generation.[9]
- As noted below, PJM is moving forward on requiring dual fuel capability at all Black Start Units but urges, as the next step, coordination across the nation of a consistent means to determine Critical Restoration Units and the development of criteria to assure fuel capability to such Critical Restoration Units.[10]
- RTOs, as part of their restoration role, should be asked to demonstrate steps they are taking to improve coordination with other critical interdependent infrastructure systems *(e.g.*, telecommunications, water utilities) that (i) could be impacted through events of type discussed herein, or (ii) are themselves vulnerabilities that could contribute to, or amplify the impact of such events. Coordination between the Commission, the Federal Communications Commission ("FCC") and DHS would provide additional federal support for such efforts.

PJM stands ready to work with the Commission and its stakeholders on each of these potential initiatives, and appreciates the Commission's leadership in this important area.

The CHAIRMAN. Mr. Ott, thank you and thank you for the reminder that as we speak we have some truly, everyday heroes that are down in the southern part of the country, in Florida and in Georgia and the Carolinas and all that region, Louisiana, that are working very hard and very diligently to keep power on. I don't think those men and women who are in the thick of the disaster—their homes are in jeopardy, their families are in fear, and they are out working to ensure that there is that support there. So thank you for recognition, and I think we all share that appreciation.

Mr. Torres, welcome to the Committee.

STATEMENT OF JUAN TORRES, ASSOCIATE LABORATORY DIRECTOR FOR ENERGY SYSTEMS INTEGRATION, NATIONAL RENEWABLE ENERGY LABORATORY

Mr. TORRES. Thank you.

Chairman Murkowski, Ranking Member Cantwell, members of the Committee, I want to thank you for this opportunity to discuss the importance of blackstart and the significant role it plays in ensuring that our power system continues to be safe, reliable and resilient.

I'm Juan Torres, and I serve as the Associate Laboratory Director for Energy Systems Integration at the U.S. Department of Energy's National Renewable Energy Laboratory, or NREL, in Golden, Colorado.

I've been affiliated with federal research in our national laboratory system for more than 28 years. In my current position, I direct NREL's efforts to strengthen the security, resilience and sustainability of our nation's electric grid.

In addition, I'm Vice Chair of the Department of Energy's Grid Modernization Laboratory Consortium, or GMLC, and I'm also team lead for the Consortium's Security and Resilience Technical Area.

I commend the Committee for this timely discussion for what I know to be a critical and central issue facing our national utility infrastructure. It's a critical concern because the economic and social impacts of a major system outage can be catastrophic.

In 2003, I oversaw a research team that investigated what came to be known as the Northeast Blackout which you mentioned in your introduction.

Simply put, blackstart is a process of restarting the power system after a system-wide blackout; however, the blackstart process is not so simple. It relies upon established procedures and trained personnel for coordinating restart of specifically designated resources to energize the transmission system, bring on other generators and get the entire system back up and running.

Restoration of the bulk power system from a blackout can be an intricate and multifaceted endeavor fraught with potential unforeseen technical challenges that are unique to each specific outage scenario. For example, history has shown that severe weather or other events may cause a simultaneous loss of more than one major grid element such as a power plant or transmission lines. Grid operators must assess each situation so that they are fully confident the set procedures will work as planned and the power system will be restored as quickly as possible.

While the concept of blackstart is well established, we need assurance that blackstart functionality is appropriately considered as the grid architecture, technology, operations and generation portfolio continue to evolve.

The DOE has taken a forward-looking approach, in partnership with utilities, to research how we can avoid catastrophic outage, as well as explore how new grid modernization technology investments might be used to provide blackstart capability. Let me provide some examples.

Under the Solar Energy Innovation Network, funded by the DOE's Solar Energy Technologies Office, NREL is working with PJM, the National Association of Regulatory Utility Commissioners and nine teams to explore blackstart applications for solar energy generation with storage. We've also—several GMLC-funded projects with relevant research. One particular project led by NREL, called Grid Frequency Support from Distributed Inverter-Based Resources in Hawaii, explored how distributed energy resources can help restore grid stability following major events such as a loss of a major power plant or transmission line. Another project led by Los Alamos National Laboratory, titled Extreme Event Modeling, is quantifying the risk of extreme events prior to an occurrence. A project led by Lawrence Livermore National Laboratory, called CleanstartDERMS, is developing a distributed energy management system that will demonstrate the start of a microgrid following an outage. More research like this is needed so we can better understand the potential for using these technologies for broader blackstart applications.

Because there are cyber threats to our power system, it is also important to consider the effects that a major cyberattack may have on system restoration. Additionally, the topic of blackstart from a cyber-induced outage is an opportune area for research by our national laboratories. Cybersecurity must be incorporated into every aspect of blackstart planning and execution.

Our ability to bounce back from a widespread power outage depends on what must be a broadly coordinated effort in partnership with all relevant stakeholders. As our power grid continues to evolve, it will be critically important to assure that our blackstart procedures remain congruent with the grid modernization investments and that they are exercised in context of the evolving spectrum of threats.

Thank you for the privilege to address this Committee.

[The prepared statement of Mr. Torres follows:]

Prepared Statement of Juan Torres
Associate Laboratory Director for Energy Systems Integration
National Renewable Energy Laboratory

For the U.S. Senate Committee on Energy and Natural Resources

October 11, 2018

Chairman Murkowski, Ranking Member Cantwell, members of the Committee, thank you for this opportunity to discuss the importance of blackstart and the significant role it plays in ensuring that our power system in the United States continues to be safe, reliable, and resilient.

I am Juan Torres, and I serve as the associate laboratory director for Energy Systems Integration at the U.S. Department of Energy's (DOE's) National Renewable Energy Laboratory, or NREL, in Golden, Colorado. I have been affiliated with federal research and our national laboratory system for more than 28 years. In my current position, I direct NREL's efforts to strengthen the security, resilience, and sustainability of our nation's electric grid. In addition, I am vice chair of the DOE Grid Modernization Laboratory Consortium (GMLC) and team lead for the GMLC's security and resilience team. The GMLC is a partnership of 13 national laboratories to advance the modernization of the U.S. power grid. Prior to joining NREL, I served for many years in various technical and managerial roles at Sandia National Laboratories advancing cybersecurity, energy, and power grid research, most recently as deputy to the vice president for energy programs. Earlier in my career, I also served on the DOE task force that developed a plan to protect U.S. energy infrastructure in response to Presidential Decision Directive 63 on Critical Infrastructure Protection.

What Is Blackstart?

Simply put, blackstart is the ability to restart the power system in the event of a blackout. The blackstart process relies on an established process for coordinating the restarting of specifically designated resources to energize the transmission system, bring on other generators, and get the entire system back up and running.

Throughout my career, I've developed a keen appreciation of the role blackstart concepts may play in the operation of a safe, reliable, and resilient electric grid. That's because the

economic and social impacts of a major system outage can be catastrophic. The Northeast Blackout of 2003, for instance, affected some 55 million residents of the United States and Canada. It is estimated to have cost some $6 billion, with at least 11 lives lost. After this event, I oversaw researchers called upon to investigate the cause of the blackout.

From the operator's perspective, blackstart is the fundamental ability to recover from a blackout by systematically bringing up essential parts of the power system *without* having an outside electrical supply available to help. It may include having the ability of a generation unit to remain operating at reduced levels when disconnected from the grid. To restore the generation of electricity after a widespread outage, blackstart configured generators must be started individually and gradually reconnected to each other. The remaining generators not configured for blackstart then synchronize themselves to the blackstart generators until the interconnected system regains full operation and all loads can be served.

In the reality of field operations, however, restoration of the bulk power system from a complete or partial blackout can be an intricate and multifaceted endeavor, fraught with potential technical challenges. To prepare for system restoration, the correct level of blackstart resources must be available at the right locations within the grid so that operators have confidence the set procedures will work as planned and time to full restoration is minimized. History has shown severe weather or other events may cause the simultaneous loss of more than one major grid element, potentially complicating a blackstart restoration. Additionally, the lack of clear, effective, and uniform policies to adequately compensate providers of blackstart resources has been identified as an important missing piece in optimizing blackstart capabilities nationwide.

The evolution of the grid from a system based largely on centralized generation to a more dynamic system with active loads, energy storage, distributed generation, and variable resources such as solar and wind only adds to the complexity involved. The good news is that these new resources, while adding new challenges, also may offer new options to help restore the grid from a blackout. That is, of course, only if the needed blackstart research and development is conducted to make that possible and adequate resources are directed to deploy and operate these new applications.

It is important to note the important role the North American Electric Reliability Corporation (NERC) plays in regulating power restoration. NERC has long-set mandatory reliability standards for Emergency Operations and Preparedness, which include restoration and blackstart procedures. The NERC standards most applicable to blackstart are detailed in sections concerning emergency operations planning, system restoration from blackstart resources, and system restoration coordination. Broadly speaking, these standards require transmission and generation operators to ensure that

their plans and designated facilities are technically sound, that control rooms are prepared to use identified restoration resources, and that personnel are appropriately trained and certified in operating principles and ready to effectively coordinate a blackstart restoration process.

Research Needed for Blackstart Capability

While the concept of blackstart is well established, considerable research is needed to ensure that blackstart functionality is appropriately considered as the grid architecture, technology, operations, and generation portfolio continue to evolve. DOE is taking a forward-looking approach and evaluating how a variety of new technologies can be used to provide blackstart capability. This includes an assessment of local energy storage, microgrids, and other distributed energy resources. Technological and operational strategies to raise the detection and situational awareness of potential brownouts and blackouts, and circumventing or mitigating those, is an additional area deserving of research.

In support of the Defense Critical Infrastructure Program (DCIP), which includes U.S. Department of Defense efforts to identify, prioritize, and coordinate the protection of critical Defense Industrial Base assets, DOE will be exploring blackstart needs to support these assets. A spectrum of generation technologies, fuel sources, and grid configurations will be encountered to meet site-specific DCIP needs, underscoring the need for robust technical and operational solutions founded on strong research and development.

Grid Modernization

As a leader of the GMLC, I understand the role that research must play in our broader grid modernization efforts. Toward that end, DOE has invested in GMLC research to increase grid reliability and resilience. One particular project led by NREL, Grid Frequency Support from Distributed Inverter-Based Resources in Hawaii, explored how distributed energy resources can help restore grid stability following major events, such as the loss of a major power plant or major transmission line. Another project led by Los Alamos National Laboratory, titled Extreme Event Modeling, is quantifying the risk of extreme events prior to an occurrence. Recently, DOE awarded several projects focused on resilient distribution systems. One of these projects, called CleanstartDERMS, was granted to Lawrence Livermore National Laboratory and includes partners Pacific Northwest and Los Alamos national laboratories. The goal is to demonstrate the use of distributed energy resources to maintain resilience on the grid to large-scale disruption events. The project will also demonstrate the potential of DER-based microgrids to serve as critical brown- and blackstart-capable resources.

The DOE Office of Electricity Delivery and Energy Reliability recently received budget approval for a particularly forward-looking project called the North American Resilience Model, or NARM. Through this project, NREL and other national laboratories will be collecting data and developing new approaches to plan and operate the grid under extreme events. This is one of the first projects of its kind to take a more complete, all-hazards approach in understanding threats and consequences. The electric grid and other vital sectors such as transportation, gas, and water are highly interdependent. Only through fully understanding these interdependencies will it be possible to plan and mitigate potential risks with analytically driven investment. NARM will look beyond electricity reliability to quantify resilience needs and compare the risk mitigation architecture and actions, including blackstart, for the electric grid—and its vital connected infrastructure.

Renewable Resources, Distributed Energy, and Energy Storage

The expansion of renewable energy technologies such as wind and solar has been considerable in some regions of the country. These technologies are playing an increasingly important role in supplying power to the grid, but we need to learn more about how they may contribute to blackstart planning and other reliability services. Though variable generation technologies such as wind and solar have not traditionally been considered part of the blackstart generation portfolio, when paired with local energy storage, these renewable technologies could be potential assets we can employ to restart the grid after a blackout.

My own research institution, NREL, currently is undertaking blackstart research under the Solar Energy Innovation Network, funded by the DOE Solar Energy Technologies Office. Our lab is working with nine teams around the country. PJM, the regional transmission organization covering 13 states and the District of Columbia, and NARUC, the National Association of Regulatory Utility Commissioners, are leading a team focusing on blackstart applications for solar energy generation with storage. PJM has stated that it is looking into blackstart applications because they are seeing a significant increase in photovoltaic generation and storage in their territory, and they believe these assets may be able to provide system resilience and effective blackstart and system restoration.

NREL likewise is studying several other key aspects of these issues, including an examination of utility experiences with, and known pilot projects for, solar energy plus storage for use in blackstart situations. This work encompasses an assessment of the technical capabilities of photovoltaics plus storage systems and an evaluation of how

solar with storage may be able to play anything from a minor role in kick-starting a larger generator to a major role in performing the complete blackstart function as a conventional generator would. Relevant business model and compensation issues are being considered as well.

Additional research is also warranted regarding the role wind power may play in blackstart. With new, more efficient control systems, the output power of wind farms can be constant in the moment, which makes it possible for wind farms to participate in power system restoration. Because of wind variability, however, the actual dispatchable output power may not always be constant. More research is necessary to better understand how to optimize the dispatch of wind farms participating in power system restoration.

Energy storage technologies are currently used in blackstart planning and execution, and their role will likely increase with technology advancements and cost reduction. These technologies are varied, including batteries, flywheels, and pumped hydro systems. Additional blackstart applications for energy storage and other distributed resources are beginning to be seriously evaluated, but more research is indicated to optimize their use.

Microgrids

Microgrids present a great opportunity for America's energy resilience strategy. They offer flexibility, local control, and resilience that the larger grid can't provide alone. And in cases of natural disaster or cyberattack, microgrids can act as energy islands, mitigating outages and quickly restoring power to critical facilities, such as hospitals and military installations. With proper planning, microgrids can also be used to provide blackstart service to distribution and transmission systems; however, while microgrids' benefits are considerable, their deployment has been uneven. High capital cost due to lack of standardization and interoperability, deployment times, and the absence of commonly understood business models are some of the roadblocks slowing their broader adoption.

Researchers at NREL and other national laboratories are engaged in advanced scientific research of microgrids. This research includes everything from fundamental research to evaluation, design, and decision support to improve their cost-effectiveness and efficiency, reduce deployment time, and continue to advance technological innovation. This work to advance microgrids directly supports national grid resilience, security, and modernization goals.

Cybersecurity and Communications

In light of the increasing cyber threat to power utilities, it is important to consider the effects that a large-scale cyberattack may have on system restoration. NERC has developed Critical Infrastructure Protection, or CIP, standards as a risk-based approach to protect the bulk grid from physical and cyberattack. While CIP standards are used to increase security against cyberattacks, we are just beginning to understand the multitude of potential ways cyber-related disruptions may impact system restoration.

To evaluate potential extreme conditions and how utilities will respond, last November NERC conducted its fourth biennial grid security and emergency response exercise, GridEx IV. With 6,500 individuals and 450 organizations participating across industry, law enforcement, and government agencies, GridEx IV was a widely represented, two-day drill, with a separate executive tabletop exercise on the second day. These exercises evaluated response scenarios to malware attacks on grid operations as well as focused cyber- and physical attacks on both generation and transmission facilities. This provided the most comprehensive simulated opportunity to date for critical electricity sector stakeholders to evaluate the effectiveness of their planned responses to cyber- and physical attacks and formulate new and more effective strategies; however, this event does not exercise blackstart from a cyber disruption.

We have come to understand that because potential cyberattacks create many serious hazards across the electric grid, cybersecurity is a primary issue that must be adequately confronted everywhere a potential vulnerability is uncovered. That, of course, includes incorporating cybersecurity into every aspect of blackstart planning and execution. Today, blackstart recovery from a cyber incident is not yet well understood or properly tested. This is an opportune area for research by our national laboratories and others.

With increasingly sophisticated communications tools dominating the way we control today's electric grid, these advanced electronic control mechanisms become even more critical when we need to effectively recover from a power blackout. Here again, these emerging technologies offer both challenges and opportunities as they pertain to blackstart concepts and planning. Intricate communications and control systems demand their own commensurately intricate responses during power recovery conditions. At the same time, SCADA (supervisory control and data acquisition) systems and wide-area measurement systems, along with artificial intelligence technology, could help us achieve self-healing of bulk power systems in the future if we devote the necessary research to this effort; however, it may still be necessary to have some level of manual blackstart capability in the event of a catastrophic cyberattack on the power grid.

Procurement and Workforce Issues

Some of the most crucial needs for improving blackstart functionality across the power grid concern procurement and compensation issues, not only technology. Unlike other ancillary services, blackstart capabilities are generally not procured through a competitive market. And while the conditions for qualification, testing, and deployment of blackstart services are spelled in various reliability plans and business manuals, there are not uniform protocols for determining what needs to be procured and how and when it should be. The poorly defined nature of blackstart service procurement is another area of needed analysis. Furthermore, while growing microgrid, wind, and solar resources may be capable of providing restoration services, they have not been required to meet the existing performance criteria requirements established for more traditional resources.

The utility industry's aging workforce, combined with a limited pool of qualified replacements, may impact our power restoration and blackstart progress as well as our broader grid modernization priorities. According to a survey by DOE, 72% of energy employers report difficulties in finding the right talent. That problem is only compounded given the increasing levels of technical proficiency these jobs are demanding. One result: the loss of trained personnel who are proficient and experienced in blackstart restoration.

In Summary

Our ability to bounce back from threats to the nation's electric grid infrastructure depends on coordinated planning, investment, and operational standards. Additional research is needed to identify the hazards before us and their mitigations. In the end, recovery is not only about shocking the system with energy; it is about conditioning the system in a coordinated way over a specified time to return it to the normal state.

As the power generation system continues to evolve, it will be critical to expand blackstart procedures and testing from not only centralized generation on the bulk power grid but also including support from renewable generation and distributed generation systems, where appropriate. Additionally, we must maintain a highly qualified workforce that is not only educated and trained but also exercised to meet the needs of an evolving power grid.

The CHAIRMAN. Thank you, Mr. Torres.
Ms. Ditto, welcome.

STATEMENT OF JOY DITTO, PRESIDENT AND CEO, UTILITIES TECHNOLOGY COUNCIL

Ms. DITTO. Chairman Murkowski, Ranking Member Cantwell and members of the Committee, I would also echo the sentiments expressed already about Hurricanes Michael and Florence and the crews there as well as the people affected by that storm, and we wish them Godspeed.

I'm extremely honored to testify today. I would like to begin by asking a few rhetorical questions. How many people know that utilities operate their own sophisticated telecommunications networks and have done so for over 70 years? And how many know that these networks are integral to the reliability and resilience of the electric grid, including the careful and delicate process of restoring power after a widespread outage? Finally, how many people know that policies made by an agency, the Federal Communications Commission, seemingly unrelated to the oversight of the electric grid, can, in fact, impact its reliability and resilience?

Even having represented electric utilities for 15 years at the time I became UTC's CEO, I didn't fully appreciate the key nature of communications to grid performance. It's become clear that many regulators, government agencies and stakeholders lack the understanding of both the communications networks deployed by utilities and the policies undermining their ability to maintain reliability. The need for such understanding is greater than ever as the industry faces numerous threats, both natural and manmade.

The cybersecurity threat is increasing at the same time the government and the public require greater levels of reliability and flexibility from an electric grid that underpins our modern way of life. The government-electric sector partnership that has emerged to combat these threats has already improved recovery and response efforts. This special relationship between the electric industry and the Federal Government to prepare, plan for and respond to disasters is only mirrored in a few other critical infrastructure sectors.

Yet, the FCC equates the electric sector with any other commercial enterprise. This disconnect must be rectified. UTC believes that it can be through greater education and collaboration among regulatory agencies such as the FCC and the Federal Energy Regulatory Commission.

UTC has a 70-year-old history representing utilities on their deployment of reliable and resilient communication systems. Most of our 200 core utility members are electric utilities of various sizes, including investor-owned, publicly-owned, cooperatively-owned and even federally-owned. All our members either own, maintain and/or operate extensive internal communication systems to help ensure the safe, reliable and secure delivery of their essential services.

Such communications networks also enable the higher levels of granularity needed to balance the electric grid as variable energy resources and other cutting-edge technologies have emerged. Utilities' private telecommunications networks are a combination of

both wired and wireless technologies. Since the '80s, utilities have also used SCADA, a type of industrial control system that transmits data over utility networks from the field into a control center. Utilities have more recently deployed a variety of new technologies on their systems to enhance situational awareness and improve efficiency, reliability and safety.

As FERC and NERC's recent reports on grid resilience have illustrated, utility communications are key to their ability to return energy to the grid after a system-wide blackout. UTC agrees with the finding in these reports.

They also highlight the investments utilities have made to ensure reliable communications during system-wide blackouts. For example, utilities prepare for the possibility of losing SCADA or other critical data communications. In such cases, they can default to voice communications. Typically deployed via push-to-talk radios, like those used by firefighters and police officers, these more basic systems can help enable the carefully coordinated blackstart processes.

Like any wireless network or device, utilities' wireless systems need radio frequency spectrum to function. Interference, which is caused by too much wireless traffic in a band, can disrupt signals, potentially disabling a critical wireless transmission. Therefore, access to adequate and interference-free spectrum is essential.

Spectrum policy resides at the FCC, the oversight of which, I realize, is outside of this Committee's jurisdiction. However, utilities' access to interference-free spectrum is integral to the provision of reliable electric service. Unfortunately, several proceedings are pending at the FCC that threaten electric reliability and resilience; one would open the 6 GHz spectrum band to unlicensed mobile users subjecting utilities, railroads and public safety to potentially harmful interference.

It's time for the FERC and the FCC to hold discussions about the growing interdependencies between the energy and telecommunications industries. Such meetings will build understanding between the two agencies and the industries they regulate. UTC urges this Committee to take a leading role in initiating such a dialogue.

Thank you for this opportunity to testify and I look forward to answering any questions you may have.

[The prepared statement of Ms. Ditto follows:]

Statement of Joy Ditto,
President and CEO,
Utilities Technology Council

Before the
Senate Committee on Energy and Natural Resources,
Hearing to Examine Blackstart

October 11, 2018

Chairman Murkowski, Ranking Member Cantwell, and Members of the Senate Energy and Natural Resources Committee:

Thank you for the invitation to testify on examining blackstart--the process of returning energy to the power grid after a system-wide blackout. Given the impact Hurricane Florence had along the Southeast and Mid-Atlantic, this is an incredibly timely hearing. I want to take a moment to commend the hard-working men and women of the utility industry who have assisted in the restoration of electricity in the wake of the storm, often in dangerous circumstances. As my testimony will detail, utility workers are among the first on the scenes after a devastating storm, restoring, repairing, and, when necessary, rebuilding utility infrastructure to bring power back on safely. Without our dedicated crews of utility workers, we would be unable to rebuild and return to normalcy. Many workers are still on the job in the aftermath of the storm, and I wish to convey my appreciation for their sacrifice.

My name is Joy Ditto and I am President and CEO of the Utilities Technology Council (UTC). I am honored to appear before you today to discuss the critical issue of returning energy to the power grid after a system-wide blackout. It is my hope that we never have to experience such a scenario, but the industry knows it must be prepared for the worst, whether it be a catastrophic storm, a physical attack, a cyberattack, or a combination of two or three of these threats. As my testimony details, the utility industry is deploying different levels of technology to make their infrastructure stronger, more robust, more resilient, and more responsive to customer demands. Most, if not all, of these enhancements are enabled by the information and communications technology (ICT) networks built, owned, and/or managed by utilities themselves. Utilities deploy their own ICT networks to assist in storm response and recovery, manage the reliability of the Bulk Electric System[1], deploy distributed energy resources, and to enable utilities to recover from so-called catastrophic "Black Sky" events.

The Utilities Technology Council (UTC) sits at the nexus between the energy and telecommunications sectors. Established in 1948, UTC is the Washington-based global association representing electric, gas and water utilities on their needs related to the deployment of reliable and resilient ICT systems. The majority of our core members[2] are electric utilities of all sizes and ownership structures, ranging from large investor-owned utilities that serve millions of customers across multi-state service territories to smaller cooperatively-organized and public power utilities that may serve only a few thousand customers. We also represent some natural gas-only and water utilities. What our members have in common is that they all either own, maintain and/or operate extensive internal communications systems that they use to ensure the safe, reliable and secure delivery of essential electric, gas and water services. Such networks, and the technologies they empower, are critical to ensuring reliable utility service and prompt restoration.

[1] As defined by FERC, the Bulk Electric System refers to all transmission elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electric energy. https://www.nerc.com/pa/RAPA/BES%20DL/bes_phase2_reference_document_20140325_final_clean.pdf
[2] See addendum

They also enable the higher levels of granularity required to balance the electric grid as distributed energy resources and other cutting-edge technologies sought by customers become more prevalent at both the Bulk Electric System level and the edge-of-the-grid distribution level.

Utility Private ICT Networks

My written testimony this morning is focused on two central elements related to today's hearing: the criticality of utility ICT networks and how these networks support the process of returning power to the grid after a system-wide blackout. First, I will briefly detail how and why utilities build and operate their own communications networks. UTC was founded in 1948 as utilities began expanding their service territories during the post-World War II economic boom. As utility lineworkers put up transmission and distribution towers, they needed telecommunications networks—often wireless, land-mobile radio push-to-talk devices—to communicate with each other. Given the inherent dangers of working with electricity, these networks needed to be as reliable—if not more so—than the electric power systems they were building. Indeed, if a utility worker needs to know whether a power line on the ground is electrified, the only way to find out is by communicating with another worker. If that communication fails, the consequences can be life-threatening.

It is important to explain the term "private network." A utility "private network" means the utility itself owns the network, rather than it being owned by a telecommunications provider. Instead of contracting out with the telecommunications industry, utilities hired their own engineers and technicians to build out their systems themselves. There are situations where utilities do partner with the telecommunications industry for elements of their ICT networks, often by leasing lines. Additionally, most utilities use telecommunications providers for their public-facing "corporate" or "enterprise" IT network needs (websites, telephone services). While these services are important, they are not tied to the reliability of the electric, gas, or water systems. Private networks are used to support utility operational technology (OT) networks and to communicate with personnel in the field.

New Technologies/Utility 2.0

Utilities have operated private networks – including wireless and wireline communications systems – for decades. Initially, these private networks were used for voice communications, but over time, data traffic on the networks increased as utilities implemented Supervisory Control and Data Acquisition (SCADA) systems to remotely monitor and control their infrastructure. In order to support their increasing communications needs, utilities began increasing the capacity of their networks, deploying fiber and microwave radio technologies. Today, utilities use private networks for a variety of applications that help to protect the grid from faults and deliver energy and water services safely and effectively. These applications include:

- Real-time monitoring of medium and high-voltage networks
- Protective relays
- Energy management
- Outage management
- Distribution management
- Smart metering
- Substation automation[3]

Utility ICT networks are characterized by high reliability and low latency to enable utilities to monitor and control operations in real-time. For example, if there is a fault, it can be quickly isolated and power can be rerouted, thereby avoiding widespread and extensive outages and damage. At the same time, utility

[3] UTC Utility Network Baseline Report 2017

networks continue to support voice communications with personnel in the field, facilitating safe, reliable and secure energy and water operations, maintenance and restoration.

Resilience of Utility ICT Networks

Utility crews must remain in constant communication when restoring power, so their ICT networks are built to withstand and quickly respond to the most severe weather and other disasters, even when electricity is out of service across a wide area. In fact, there have been multiple occasions, including Hurricane Katrina in 2005, when commercial telecommunications providers used utility ICT networks to bring their own communications systems back online after a disruptive event.[4] A recent example of the resilience of these networks came this past March, when a powerful storm brought intense and prolonged winds to the Northeast and Mid-Atlantic. Named Winter Storm Riley, the storm left approximately 1.9 million customers without electricity between March 1-3, from Virginia all the way up to New England. The storm generated frequent wind gusts from 70-90 MPH, and the Washington area experienced sustained winds of nearly 50 MPH for nearly 12 hours.[5]

Yet utility ICT networks remained functional throughout the storm, allowing for the prompt restoration of electricity when it was safe to do so. UTC member Rappahannock Electric Cooperative, a cooperative utility serving parts of Northern and Central Virginia, experienced power outages to 71,246 customers. The storm broke 350 of its utility poles and caused $3.65 million in damages. The utility's territory faced wind gusts up to 78 MPH for nearly half a day. However, its ICT networks sustained minimal damage. Its microwave communications system had three dish antennae blown off of their directional path by the wind gusts, but overall service was not impacted.

Four "Buckets" of Utility ICT Networks

There are four main "buckets" or categories of uses for private utility ICT networks. They are: normal, day-to-day "Blue Sky" operations; hazardous weather, "Grey Sky" operations; catastrophic, unanticipated "Black Sky" events; and utility 2.0/edge of the grid, futuristic operations.

Normal, Blue Sky operations refer to the day-to-day reliable operation of a utility's infrastructure. This generally means moderate temperatures resulting in manageable load/demand expectations, with no weather, cyber, or physical incidents or emergencies. On these "normal" days, utilities use their ICT networks for a host of operations as illustrated in the list above. Even when temperatures are moderate and load is easily met, utility ICT networks are essential to the reliable operation of the grid.

These systems are even more critical in "Grey Sky" operations. Grey Sky refers to what we most recently experienced with Hurricane Florence— in which a utility faces severe weather or other incident causing widespread outages. Hurricane Florence, for example, resulted in approximately 1.9 million temporary power disruptions. Utility crews were able to communicate even when the power was out, allowing them to make repairs and restorations as safely as possible. They were able to do this because they invested extensively in back-up power for their communications towers and other communications sites.

A Black Sky event is something else entirely. Black Sky operation refers to catastrophic events compromising electric reliability and the country's collective effort to respond and restore service, possibly resulting in long-term power disruptions. The reason for such an event could be from a devastating natural disaster, cyberattack, physical attack, act of war, or a combination of incidences. The resulting impact could mean a utility is unable to restore service safely for numerous reasons, including the failure of utility ICT networks. Generally speaking, these are events in which there is little to no

[4] https://transition.fcc.gov/pshs/docs/advisory/hkip/presenters060130/p06.pdf
[5] https://weather.com/storms/winter/news/2018-03-01-winter-storm-riley-noreaster-high-winds-coastal-flooding-heavy-snow

warning, meaning government and industry do not have much time to prepare and implement restoration plans in advance.

The fourth bucket of utility ICT network use is the onset of edge-of-the-grid technologies. Distributed energy resources, smart meters, and many Industrial Internet of Things applications cannot function without ICT networks. Battery storage, rooftop and community solar and other distributed energy resources all require utility communications networks. Otherwise utilities would be unable to balance load with the appropriate resources to keep the lights on and maintain the integrity of the grid. Although these initiatives are largely within the jurisdiction of state and local regulatory authorities, they underscore the need for reliable and resilient utility ICT systems.

Blackstart
The subject for today's hearing is the ability of the utility industry to return energy to the grid after a system-wide blackout. For reference, the Federal Energy Regulatory Commission (FERC) and North American Electric Reliability Corporation (NERC) issued a May joint report called "FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans." This report focused on "Blackstart Resources Availability (BRAv)." This report the most recent in a series of joint FERC-NERC studies into the restoration and recovery of the Bulk Electric System from a widespread, prolonged outage or blackout.[6]

Blackstart refers to specific generating units that are used to return power after a massive blackout. The May 2018 FERC-NERC study evaluated blackstart resources and planning by nine utilities subject to NERC regulations. The report notes that, while some utilities have seen a fall in the availability of blackstart resources due to retirement of blackstart-capable units over the past decade, they have identified sufficient resources in their system restoration plans, and have developed comprehensive strategies for mitigating against future loss of any additional blackstart resources.[7] In addition, the report found that the utilities have performed expanded testing of their blackstart capabilities and update and modify their system restoration plans over time.[8]

ICT Networks during Blackstart
As we have already discussed, utility private ICT networks are essential to reliable utility operations in all situations, especially during times of system restoration, repair, and recovery, including the coordination of blackstart generation units to bring power back online after massive outages. The FERC-NERC reports indicate that utilities perform regular testing of their communications systems to ensure they can operate whether faced with a powerful hurricane which could take out power for days or a crippling cyberattack. Utility crews must be able to communicate with each other no matter the circumstances to safely return electricity to the grid -- a delicate, multi-step process. If not done safely and carefully, this process could jeopardize the safety of the utility crews in the field and further damage the grid.

For example, in a June 2017 joint FERC-NERC "Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans," the Commission and NERC worked with eight volunteer registered NERC entities to gauge how they could operate in situations where their communications are compromised during a blackout. The report envisioned a scenario of utilities losing the operation of the SCADA systems and whether and how these utilities would be able to restore service in such a state. The report found that all of the participating entities have protocols in place should this kind of event take place.

---

[6] https://www.ferc.gov/legal/staff-reports/2018/bsr-report.pdf?csrt=9677689259104373 5
[7] https://www.ferc.gov/media/news-releases/2018/2018-2/05-02-18.asp#.W5gWE0xFwXK
[8] https://www.ferc.gov/legal/staff-reports/2018/bsr-report.pdf?csrt=967768925910437 35, page 2

"Overall, the joint study team found that participants have made significant investments to help ensure their normal means of communications are available during blackout events to support the system restoration process, including taking steps to ensure expedited restoration of vital communications and data transfer systems, e.g., through implementation of Telecommunications Service Priority. However, similar to their approach for the potential loss of SCADA, all participants also prepare for the possibility that their normal means of communications may be partially or totally unavailable at some time during a restoration event through the provision of alternate and backup forms of communication."[9]

This study also found that the volunteer utilities "have multiple forms of interpersonal communications between system operators/control centers" and reliability coordinators, blackstart generators, other generation plants, field personnel, and neighboring system operators.[10]

Moreover, in its May 2018 report, FERC-NERC point to communications as a critical function of restoring service during a prolonged outage. The report again notes that utilities perform rigorous testing to coordinate their communications systems at higher levels and intervals than as required by FERC-approved reliability standards.[11]

> "For instance, prior to performing expanded testing, the transmission operator typically notifies the reliability coordinator about the date and time of the test and seeks approval for the test. In some regions, the reliability coordinator monitors the entire test. If customer outages are necessary for completing the test, the affected customers are notified prior to testing by the testing registered entity. In some regions, registered entities may also have to be mindful of the emissions restrictions imposed on the blackstart unit and, if necessary, may have to secure the appropriate permits from regulators prior to the test. During testing, transmission operators communicate with substation personnel via radios and maintain constant communications with the generator operator at the blackstart generating unit. Field personnel deployed at substations and along transmission lines periodically communicate with each other and with control center operators. One participant who has successfully performed expanded testing requires constant communication between the control center operators and field personnel performing the tests during each stage of the test. For instance, during the energizing of transmission lines, control center dispatchers provide specific instructions to substation field personnel who perform functions such as opening and closing breakers, and report back to the dispatcher.[12]"

In addition, the May 2018 FERC-NERC joint study indicated that utilities rely on SCADA systems and other ICT network tools to monitor and control voltage, current, and frequency during this testing. "Blackstart generator operators monitor voltage at the generating unit, while transmission operators monitor and control voltage at control centers via EMS/SCADA. Some participants also monitor voltage and voltage limit exceedances at substations. One participant dispatches field personnel to substations with recording equipment to monitor voltage and to ensure that voltage limits are not exceeded."[13]

Every element of the processes described above involves utility communications. Because of the critical nature of ICT networks, utilities implement extended back up power for their ICT systems and design their networks to provide diverse routing and redundant communications to ensure reliability. These high standards are necessary to ensure that if utility communications are indeed compromised, they can be restarted quickly. Once operational, utilities can use their networks for the functions to restore service.

---

[9] FERC-NERC Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans
[10] Ibid.
[11] https://www.ferc.gov/legal/staff-reports/2018/bsr-report.pdf?csrt=9677689259104373 5
[12] Ibid.
[13] Ibid.

Utilities have added numerous advanced capabilities to their networks to assist in the restoration of service during prolonged outages. Although Hurricane Harvey in 2017 did not result in the need for blackstart services, the devastation posed significant other challenges to power restoration. For example, because of the incredible flooding from the storm, CenterPoint Energy used drones to help crews gain better situational awareness of the damage to their infrastructure, helping them prioritize service restoration. CenterPoint Energy used 15 drones in total, which enabled real-time updates and visuals into its service territory in the wake of the storm. Additionally, CenterPoint Energy said its smart-meter program reduced outages overall and made for more efficient recovery.[14]

Policy Implications for ICT Networks
As demonstrated, utility private ICT networks underpin the reliable operation of our nation's Bulk Electric System. Without them, reliability even on Blue Sky days would suffer, as utilities would not have timely, accurate information to balance generation and demand.

Utility communications networks consist of both wireline and wireless technologies. Depending on the size, location, terrain, and geography of a utility's service territory, along with the expense of laying fiber wirelines to these potentially remote locations, many utilities rely on wireless communications for substantial parts of their networks. Like any wireless network, utility ICT systems need radio frequency spectrum to function, and the reliability of the wireless communications can be affected by radio frequency interference. Because electricity is generated and consumed instantaneously, the electricity grid requires a delicate balance between supply and demand. This means that utility ICT networks must transmit data at high speeds to avoid power disruption. Radiofrequency interference to communications can displace and disrupt signals, potentially disabling the ability of a critical wireless transmission to reach its destination. Because of the critical nature of utility services, interference to mission-critical communications within their ICT networks is intolerable. Therefore, access to adequate and interference-free spectrum is required if these networks are to work as intended.

FERC-FCC Meetings
UTC has filed several statements for the record to this committee in various hearings it has held on FERC and related energy issues. In these statements, we have noted that spectrum policy resides at an agency outside of this committee's jurisdiction—the Federal Communications Commission (FCC). We have stated that the policies decided at the FCC directly impact utility operations which are overseen, in part, by FERC and the Department of Energy, over which this Committee does has jurisdiction.

The FCC manages spectrum policy under the Communications Act of 1934[15], which requires the FCC to manage spectrum in the public interest. In the Balanced Budget Act of 1997, Congress authorized the FCC to award spectrum through auction, although it also exempted utilities from competitive bidding of spectrum, given the importance of utility services to the country[16]. Despite this congressional requirement, the FCC has treated utilities the same as any other commercial entity when it comes to spectrum acquisition. As a result, utilities often find themselves unable to compete with other enterprises for interference-free spectrum. Spectrum is one of the key resources to private utility ICT networks, which also means spectrum is essential to the reliability of our nation's Bulk Electric System.

---

[14] http://www.ercot.com/content/wcm/key_documents_lists/103998/5.3.2_CenterPoint_Energy_s_Response_to_Hurricane_Harvey_REVISED_10.12.17.pdf

[15] See Communications Act of 1934, as amended, 47 U.S.C. § 151 et seq.

[16] H. Rept. No. 105-217, Section 3002(a), (1997)

Agency Cross-Coordination Needed

FERC's regulations require electric utilities to meet stringent reliability standards in order to provide the highest levels of reliable service as demanded by the government and, more importantly, the industry's customers. Integral to the utility industry's compliance with these regulations is access to interference-free spectrum. Without access to adequate interference-free spectrum, private utility networks will not be as reliable and resilient as they are now. Yet, the FCC has pending proceedings that threaten to compromise the safety, reliability and security of utility networks. One proceeding would expand access to the 6 GHz spectrum band to unlicensed users. Many utilities use the 6 GHz band for mission-critical communications, including day-to-day reliability monitoring and emergency response. Our fear is that letting new commercial users into the band will cause interference to utility mission-critical networks.

Because spectrum policy is managed by the FCC, and because the deployment of ICT networks is interwoven into the deployment of electric service, we believe it is time to hold cross-agency and cross-jurisdictional discussions between the FCC and FERC about the growing interdependencies between the energy and telecommunications industries. Such meetings would build understanding between the two regulatory bodies and the industries they regulate. On behalf of our members, we urge the Senate Energy and Natural Resources Committee to encourage the FCC and FERC to hold regular meetings. We have also made this request to Members of the Senate Committee on Commerce, Science and Transportation, Members of the House Energy and Commerce Committee, and commissioners and staff of both FERC and the FCC.

We are aware and supportive of efforts to convene high-level discussions between the industries through the various Sector Coordinating Councils, such as the Electricity Subsector Coordinating Council and the Communications Sector Coordinating Council. The industries, along with others, are developing a Strategic Infrastructure Coordinating Council (SICC) to identify mutual priorities and develop cross-sector incident response plans.[17] We believe these discussions underscore the need for FERC and the FCC to discuss the growing interdependencies between the energy and telecommunications industries. We also urge the Departments of Energy and Commerce to embrace cross-sector and cross-agency coordination through providing forums for their agencies to interact on these topics and encourage the regulatory agencies to do so.

Conclusion

Our industry's response to Hurricane Florence demonstrates the importance of this hearing. As much as we in the industry hope that we never experience blackstart events, we still must prepare for the worst. In order to do so, many utilities own and operate their own ICT networks to manage day-to-day reliability and emergency response. Utility crews maintain these systems so they can be used even when the electricity is out, as they are essential to the restoration of utility services. These networks and the technologies they enable have benefited the public by reducing outage duration and developing stronger, more resilient and nimble utility systems. Additionally, utility networks are essential for the deployment of distributed energy resources and other edge of the grid applications. The clear and growing interdependencies between the energy and telecommunications industries require more coordination between federal agencies, and we ask this Committee and others to take a leading role to make this happen.

Thank you for this opportunity to testify this morning. I look forward to answering any questions you may have.

[17] http://www.electricitysubsector.org/ESCCInitiatives.pdf?v=1.8

ADDENDUM

UTC Core Utility Membership Snapshot
(as of Oct. 5, 2018)

Investor-Owned Utilities, 57

Alliant Energy	Dubuque	IA
Ameren	St. Louis	MO
American Electric Power Company, Inc.	Gahanna	OH
AVANGRID	New Gloucester	ME
Avista Corp.	Spokane	WA
Black Hills Energy	Pueblo	CO
CenterPoint Energy	Houston	TX
Central Hudson Gas & Electric Corporation	Poughkeepsie	NY
Cleco Corporate Holdings LLC	Bunkie	LA
Consumers Energy	Jackson	MI
Dayton Power & Light Company	Moraine	OH
Dominion Resources, Inc.	Richmond	VA
DTE Energy	Detroit	MI
Duke Energy Corporation	Charlotte	NC
Duquesne Light Company	Pittsburgh	PA
El Paso Electric Company	El Paso	TX
Entergy	New Orleans	LA
Eversource Energy	Berlin	CT
Exelon Corporation	Chicago	IL
Florida Power & Light Company	Miami	FL
Hawaiian Electric Company, Inc.	Honolulu	HI
Idaho Power Company	Boise	ID
ITC Holdings Corp	Novi	MI
Kansas City Power & Light	Kansas City	MO
LG&E and KU Services Company	Louisville	KY
Louisiana Generating LLC	Baton Rouge	LA

Madison Gas & Electric Company	Madison	WI
Minnesota Power	Duluth	MN
Montana-Dakota Utilities Co.	Bismarck	ND
National Grid USA Service Company, Inc.	Syracuse	NY
Northern Indiana Public Service Company	Merrillville	IN
NorthWestern Corporation	Sioux Falls	SD
NV Energy	Las Vegas	NV
NW Natural	Portland	OR
Ohio Valley Electric Corporation	Piketon	OH
Oncor Electric Delivery Company	Dallas	TX
Orange & Rockland Utilities, Inc.	Pearl River	NY
Otter Tail Power Company	Fergus Falls	MN
Pacific Gas & Electric Company	Oakland	CA
PacifiCorp	Portland	OR
Peoples TWP	Butler	PA
Portland General Electric Company	Portland	OR
PPL Corporation	Allentown	PA
Public Service Enterprise Group	Newark	NJ
Puget Sound Energy	Redmond	WA
SCANA Corporation	Cayce	SC
Sempra Energy Utilities	San Diego	CA
Southern California Edison Company	Rosemead	CA
Southern Company	Atlanta	GA
Tampa Electric Company	Tampa	FL
United Illuminating Company	New Haven	CT
Vermont Electric Power Company	Rutland	VT
Washington Gas Light Company	Springfield	VA
WEC Energy Group	Milwaukee	WI
Westar Energy	Topeka	KS
Wolf Creek Nuclear Operating Corporation	Burlington	KS

Xcel Energy Services Inc.	Minneapolis	MN

Public Power, 51

Burbank Water and Power	BURBANK	CA
Central Lincoln People's Utility District	Newport	OR
Central Nebraska Public Power & Irrigation District	Holdrege	NE
Chelan County Public Utility District No. 1	Wenatchee	WA
City of Folsom, Environmental & Water Resources Department	Folsom	CA
City Utilities of Springfield	Springfield	MO
Cleveland Utilities	Cleveland	TN
Columbia Water & Light	Columbia	MO
Conway Corporation	Conway	AR
CPS Energy	San Antonio	TX
Decatur (TX)	Decatur	TX
East Columbia Basin Irrigation District	Othello	WA
El Dorado Irrigation District	Placerville	CA
Energy Northwest	Richland	WA
Eugene Water & Electric Board	Eugene	OR
Gainesville Regional Utilities	Gainesville	FL
Grays Harbor County Public Utility District No. 1	Aberdeen	WA
Harrisonburg Electric Commission	Harrisonburg	VA
Huntsville Utilities	Huntsville	AL
JEA	Jacksonville	FL
KCK Board of Public Utilities	Kansas City	KS
Kitsap County Public Utility District No.1	Poulsbo	WA
Lakeland (FL)	Lakeland	FL
Lincoln Electric System	Lincoln	NE
Los Angeles Department of Water & Power	Los Angeles	CA
Lower Colorado River Authority	Austin	TX
Memphis Light, Gas & Water Division	Memphis	TN
Modesto Irrigation District	Modesto	CA

Nashville Electric Service	Nashville	TN
Navajo Tribal Utility Authority	Fort Defiance	AZ
Nebraska Public Power District	York	NE
New York Power Authority	White Plains	NY
North Attleborough Electric Department	North Attleborough	MA
Omaha Public Power District	Omaha	NE
Orlando Utilities Commission	Orlando	FL
Platte River Power Authority	Fort Collins	CO
PREPA Networks	Guaynabo	PR
Regional Water Authority	New Haven	CT
Sacramento Municipal Utility District	Sacramento	CA
Salt River Project	Tempe	AZ
Santee Cooper	Moncks Corner	SC
Silicon Valley Power	Santa Clara	CA
Snohomish County Public Utility District No. 1	Everett	WA
Soquel Creek Water District	Capitola	CA
South Feather Water & Power	Oroville	CA
South Florida Water Management District	West Palm Beach	FL
Sweetwater Utilities Board	Sweetwater	TN
Tacoma Power - Utility Technology Services	Tacoma	WA
Tripp County Water User District	Winner	SD
Turlock Irrigation District	Turlock	CA

Cooperative Utilities (Distribution)

Access Energy Cooperative	Mt. Pleasant	IA
Allamakee-Clayton Electric Cooperative, Inc.	Postville	IA
Bandera Electric Cooperative, Inc.	Bandera	TX
BARC Electric Cooperative	Millboro	VA
Barry Electric Cooperative	Cassville	MO

Berkeley Electric Cooperative, Inc.	Moncks Corner	SC
Blue Ridge Electric Membership Corporation	Lenoir	NC
Brunswick Electric Membership Corporation	Shallotte	NC
Callaway Electric Cooperative	Fulton	MO
Cass County Electric Cooperative	Fargo	ND
Central Florida Electric Cooperative	Chiefland	FL
Citizens Electric Corporation	Perryville	MO
Clay Electric Cooperative Inc.	Keystone Heights	FL
Colquitt Electric Membership Corporation	Moultrie	GA
CO-MO Electric Cooperative Inc.	Tipton	MO
Consolidated Electric Cooperative, Inc. (OH)	Mount Gilhead	OH
Consumers Power Inc.	Philomath	OR
Delta-Montrose Electric Association	Montrose	CO
Diverse Power Inc.	LaGrange	GA
Dixie Electric Power Association	Laurel	MS
Dixie Power	Beryl	UT
Douglas Electric Cooperative, Inc. (OR)	Roseburg	OR
Duck River Electric Membership Corp.	Shelbyville	TN
Escambia River Electric Cooperative	Jay	FL
Excelsior Electric Membership Corporation	Metter	GA
Flathead Electric Cooperative Inc.	Kalispell	MT
Forked Deer Electric Cooperative	Halls	TN
Gascosage Electric Cooperative	Dixon	MO
Gibson Electric Membership Corporation	Trenton	TN
Habersham EMC	Clarkesville	GA
Holston Electric Cooperative	Rogersville	TN
Idaho County Light & Power Cooperative Association, Inc.	Grangeville	ID
Illinois Rural Electric Cooperative	Winchester	IL
Joe Wheeler Electric Membership Corporation	Trinity	AL

Johnson County Rural Electric Membership Corporation	Franklin	IN
Kenergy Corp.	Owensboro	KY
Lake Region Electric Cooperative, Inc. (OK)	Hulbert	OK
Lyon Rural Electric Cooperative	Rock Rapids	IA
Meriwether Lewis Electric Cooperative	Centerville	TN
Mid-Carolina Electric Cooperative	Lexington	SC
Mid-South Synergy	Navasota	TX
Midwest Energy Cooperative	Cassopolis	MI
Midwest Energy, Inc.	Hays	KS
Northern Electric Cooperative (SD)	Bath	SD
Northern Neck Electric Cooperative	Warsaw	VA
Northern Virginia Electric Cooperative	Manassas	VA
Owen Electric Cooperative Inc.	Owenton	KY
Ozarks Electric Cooperative	Fayetteville	AR
Parke County Rural Electric Membership Corporation	Rockville	IN
Pedernales Electric Cooperative	Johnson City	TX
Pennyrile Rural Electric Cooperative	Hopkinsville	KY
Plumas-Sierra REC	Portola	CA
Ralls County Electric Cooperative	New London	MO
Rappahannock Electric Cooperative	Fredericksburg	VA
Richland Electric Cooperative	Richland Center	WI
Salem Electric	Salem	OR
San Bernard Electric Cooperative	Bellville	TX
San Luis Valley Rural Electric Cooperative	Monte Vista	CO
Sequachee Valley Electric Cooperative	South Pittsburg	TN
South Central Arkansas Electric Cooperative	Arkadelphia	AR
South Central Indiana REMC	Martinsville	IN
South Plains Electric Cooperative	Lubbock	TX
Southern Illinois Power Cooperative	Marion	IL
Talquin Electric Cooperative, Inc.	Quincy	FL

Tri-County Electric Cooperative (OK)	Hooker	OK
United Electric Cooperative (MO)	Savannah	MO
Warren Rural Electric Cooperative Corporation	Bowling Green	KY
West River Electric Association, Inc.	Wall	SD
Woodbury County Rural Electric Cooperative	Moville	IA
Mille Lacs Electric Cooperative	Aitkin	MN

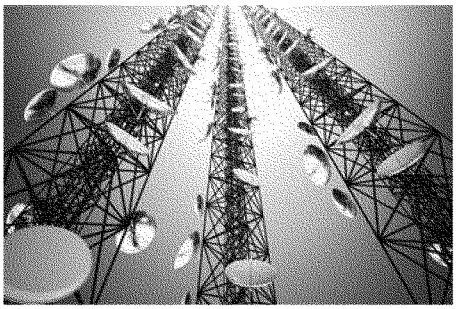
Cooperative Utilities, Generation & Transmission

Arizona Electric Power Cooperative	Benson	AZ
Arkansas Electric Cooperative Corp.	Little Rock	AR
Basin Electric Power Cooperative	Bismarck	ND
Brazos Electric Power Cooperative, Inc.	Waco	TX
Buckeye Power Inc.	Columbus	OH
Central Electric Power Cooperative (MO)	Jefferson City	MO
Central Iowa Power Cooperative	Cedar Rapids	IA
Chugach Electric Association Inc.	Anchorage	AK
Corn Belt Power Cooperative	Humboldt	IA
Dairyland Power Cooperative	LaCrosse	WI
East River Electric Power Cooperative	Madison	SD
Georgia System Operations Corp.	Tucker	GA
Great River Energy	Maple Grove	MN
Hoosier Energy Rural Electric Cooperative	Bloomington	IN
Kamo Power	Vinita	OK
M & A Electric Power Cooperative	Poplar Bluff	MO
Minnkota Power Cooperative, Inc.	Grand Forks	ND
New Horizon Electric Cooperative	Laurens	SC
Northeast Missouri Electric Power Cooperative	Palmyra	MO
Northwest Iowa Power Cooperative	Le Mars	IA
PowerSouth Energy Cooperative	Andalusia	AL

Rushmore Electric Power Cooperative	Rapid City	SD
South Texas Electric Cooperative	Nursery	TX
Sunflower Electric Power Corporation	Garden City	KS
Tri-State Generation and Transmission Association, Inc.	Denver	CO
Wabash Valley Power Association	Indianapolis	IN
Western Farmers Electric Cooperative	Anadarko	OK
Wolverine Power Cooperative, Inc.	Cadillac	MI

Utilities Technology Council™

Utilities Technology Council



Utility Network Baseline

November 2017

©2017 Utilities Technology Council

Table of Contents

Introduction and Context 3
Utility Network Baseline 5
Size of Utilities Surveyed, by Substations 5
Size of Utilities Surveyed, by Service Territory 6
Utility Networks Support Critical Functions 7
Utility Networks Transport Data That Is Critical to Reliable Energy Supply 8
Utilities Rely on Land Mobile Radios (LMR) 9
Utility Miles of Fiber Installed 10
Utility Number of Microwave Paths 11
Utility Bandwidth Needs Are Growing Quickly 12
Network Composition: Current and Medium Term 13
Fiber and Microwave Are the Dominant Network Media 14
Utilities Mainly Share Networks with Other Utilities 15
Licensed vs. Unlicensed Frequency Usage 16
Utilities Rarely Outsource Network Ownership 17
Utilities Rarely Outsource Network Monitoring 18
Carriers Do Not Adequately Prioritize Recovery of Utility Telecoms 19
Lead Time to Enable New Services 20

 © 2017 Utilities Technology Council

Introduction and Context

The Utilities Technology Council (UTC) conducted a Network Baseline Survey of its member electric, gas, and water utilities during September and October 2017 to characterize utilities' telecommunications in their critical operations. After consolidating multiple responses from some utilities, the survey has responses from 41 electric utilities, about 20% of UTC's member utility population. Respondents range from large to small utilities of all ownership types – investor-owned, public power and cooperative. The following pages present charts and brief analyses of the current state of UTC member utilities' telecommunications.

Utilities reported that their telecommunications networks support capabilities that are critical to the reliable supply of electricity, including:

- Real-time monitoring of medium and high voltage networks (distribution and transmission, respectively)
- Protective relays
- Energy management
- Outage management
- Distribution management
- Smart metering
- Substation automation

Utilities' grid modernization uses telecommunications networks and digital technology to improve reliability of supply as intermittent distributed energy generation increases. Telecommunications networks are critical to moving data between remote grid sensors and data-based decision making at utilities' central sites. Utilities need huge amounts of data from the field in order to make their power delivery more reliable and efficient. Telecommunications networks are essential to getting all of that data to the right place, at the right time. Without reliable telecommunications, grid modernization is impossible.

The survey responses show little differentiation of the telecommunications and technology requirements between large and small utilities. All are interconnected and all face similar challenges. However, large utilities have the resources to deploy sophisticated telecommunications networks, while smaller utilities may not. Large utilities easily attract the attention and support of nationwide telecommunications carriers such as AT&T, Verizon, and Sprint, even if those carriers cannot provide optimally reliable service. Smaller utilities, though facing many of the same needs, are sometimes challenged to receive adequate support from those same carriers.

 © 2017 Utilities Technology Council

Many utilities – electric, gas, and water – have chosen to deploy their own internally focused, private telecommunications networks to ensure the high levels of reliability expected by their customers and regulators. Utilities will from time to time use carrier-provided services or lease fiber and copper lines where those better fit a business case. The mix of in-house and outsourced telecommunications networks underpins the digital machine-to-machine technology that enables modern technologies to improve reliability and give utilities a big-picture vision of their networks.

 © 2017 Utilities Technology Council

Utility Network Baseline

Size of Utilities Surveyed, by Substations

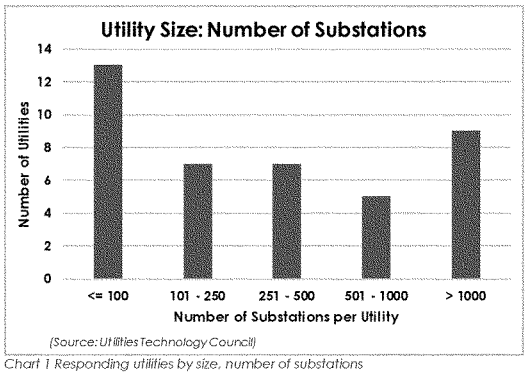


Chart 1 Responding utilities by size, number of substations

Chart 1 shows that UTC received responses from a diverse range of utilities, ranging from smaller utilities with less than 100 substations, up to larger utilities with over 1,000 substations.

As expected, nearly all the "small" substations in the distribution are smaller public power or cooperative utilities.

All the utilities with over 1,000 substations are "household name" investor-owned utilities.

Throughout this analysis, the number of substations is used frequently as a proxy for size of the utility. Later charts display particular attributes, broken down by size of utility – that is, the number of substations.

© 2017 Utilities Technology Council

Size of Utilities Surveyed, by Service Territory

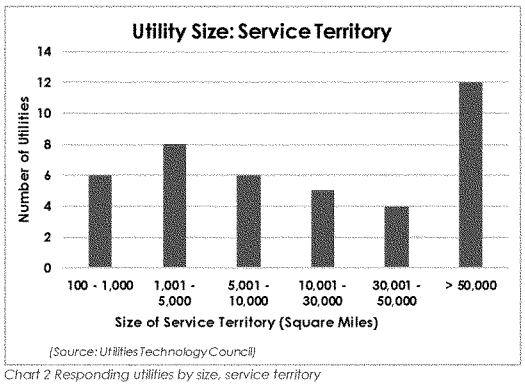


Chart 2 Responding utilities by size, service territory

Utilities also reported their approximate service territory size. This was used as an additional proxy for utility size, although a less effective proxy than number of substations.

Again, the chart shows a wide diversity of utilities when measured by size of their service area.

Among the utilities with a service territory exceeding 30,000 square miles, most had more than 1,000 substations, but a few had less than 500 substations and one utility had less than 100 substations. The last scenario is consistent with a rural utility having a large service area but a low population density.

As expected, utilities with the largest service territories tended to have the largest amount of optical fiber deployed. Large service territories also correlate to greater use of microwave (wireless) telecommunications, as shown later in Chart 7.

© 2017 Utilities Technology Council

Utility Networks Support Critical Functions

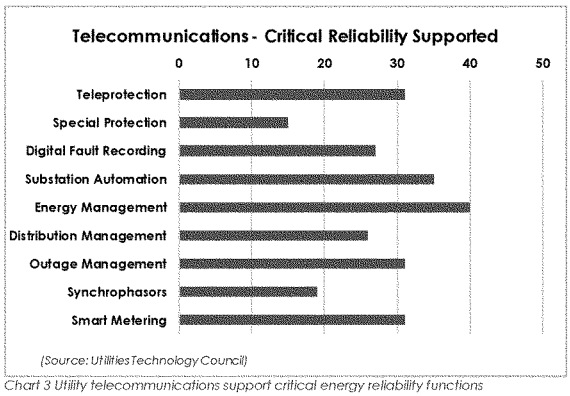


Chart 3 Utility telecommunications support critical energy reliability functions

The survey asked utilities which critical reliability functions are supported by their telecommunications networks. The typical answer was "all of the above." This chart shows some of the key capabilities supported by telecommunications.

These capabilities focus on increased reliability, decreased or eliminated outages, and improved efficiency – which together translate into more reliable energy, delivered at a lower cost. For example:

- Teleprotection is key to minimizing the impact and duration of network faults.
- Energy Management Systems optimize generation and high-voltage transmission of energy, both of which are hugely expensive operations.
- Distribution Management Systems keep neighborhood distribution grids balanced as more and more residential solar energy and other distributed generation resources are introduced into the grid.
- Smart Metering delivers a multitude of benefits, including reduced expense of recording consumption and the ability to charge consumers lower rates for off-peak energy consumption.

© 2017 Utilities Technology Council

Utility Networks Transport Data That Is Critical to Reliable Energy Supply

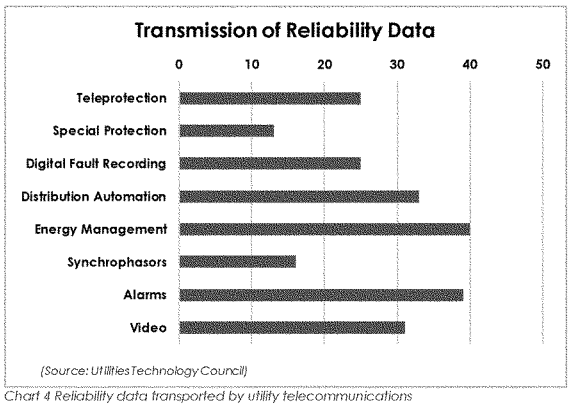


Chart 4 Reliability data transported by utility telecommunications

Much like the critical reliability capabilities described above in Chart 3, networks must transmit enormous amounts of data needed for decision-making at central sites. There, operational data from the utilities' field networks is combined with enterprise data and external inputs such as weather forecasts or even social media to determine current and near-term energy required by consumers.

The final two rows of the above chart are critical for physical protection of substations and other facilities: streaming video and alarms that are essential for reliability as utilities begin to place substantial computing and storage capabilities at unmanned substation locations.

Streaming video data rates dwarf those of any other data that utilities are likely to capture. Utilities often restrict video data to wired networks. Existing utility wireless networks are unlikely to support the bandwidth required for video data. This may be a challenge for remote substations with only wireless telecommunications connectivity, where spectrum availability and access determine bandwidth.

© 2017 Utilities Technology Council

Utilities Rely on Land Mobile Radios (LMR)

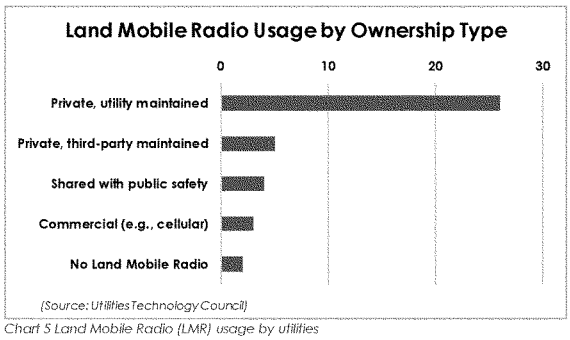


Chart 5 Land Mobile Radio (LMR) usage by utilities

Utilities rely upon their land mobile radios (LMR)--when cellular carrier service becomes unavailable during or after a natural disaster, LMR is still there. UTC member utilities that have dealt with hurricane recoveries during 2016 and 2017 reported consistently that when all else failed, they could still depend on LMR.

This chart points out two key aspects of LMR usage:

- Nearly all responding utilities use private LMR systems. In a few cases those systems are third-party maintained, but still owned by the utility.
- Only two utilities responded that they have no LMR – both small utilities.

Notwithstanding carriers' claims that their cellular services can provide the same level of reliable service as LMR, UTC expects that utilities will continue to use and possibly increase their use of LMR. LMR can provide more reliable communications than carrier services during and after disasters. Additionally, LMR can reach remote areas, where carriers may not provide coverage.

 © 2017 Utilities Technology Council

Utility Miles of Fiber Installed

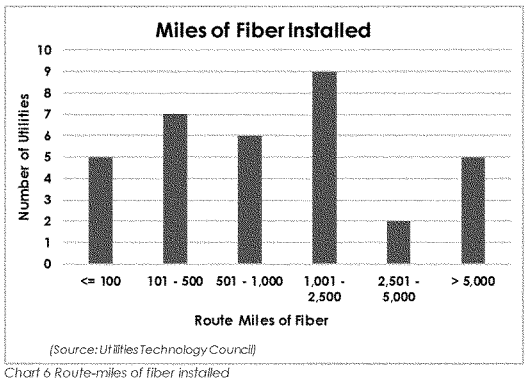


Chart 6 Route-miles of fiber installed

Chart 6 shows again the diversity of utilities that responded to UTC's survey. The utilities reporting less than 100 route-miles of fiber were all rural cooperatives that also reported a large reliance upon microwave telecommunications.

Smaller utilities with large service areas are almost forced to use wireless telecommunications because wireless microwave telecommunications are cost-effective and operate effectively over large open areas. However, diverse geographic features such as trees and terrain can render microwave deployments challenging as well.

All the utilities that reported more than 5,000 route-miles of fiber deployment are large investor-owned utilities. A recurring finding from the survey is that large utilities have invested in these often expensive but highly reliable fiber wireline buildouts, while some smaller utilities have not. Large utilities have large data bandwidth requirements and therefore need to deploy fiber even to remote substations. Several utilities have indicated that they are putting fiber on every new transmission line that they build, given their need for highly reliable telecommunications.

© 2017 Utilities Technology Council

Utility Number of Microwave Paths

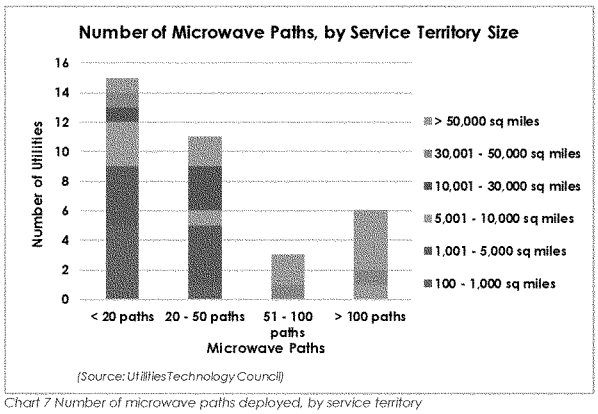


Chart 7 Number of microwave paths deployed, by service territory

Turning to wireless telecommunications, utilities of all sizes use microwave, but as the rightmost bars in Chart 7 show, larger service territories correlate to more microwave paths. This decision is likely driven by the logistics and capital expense of running fiber throughout a large service territory.

All of the utilities reporting 51 or more paths are large investor-owned utilities. Most likely this is due to the sheer amount of data that they must move and the size of their service territories.

Utilities – large or small – with lower bandwidth requirements may determine that microwave is more financially viable. When bandwidth requirements permit, microwave telecommunications may offer acceptable data transmission with less infrastructure build-out (capital expenditure) and ongoing maintenance (operational expenditure) required.

© 2017 Utilities Technology Council

Utility Bandwidth Needs Are Growing Quickly

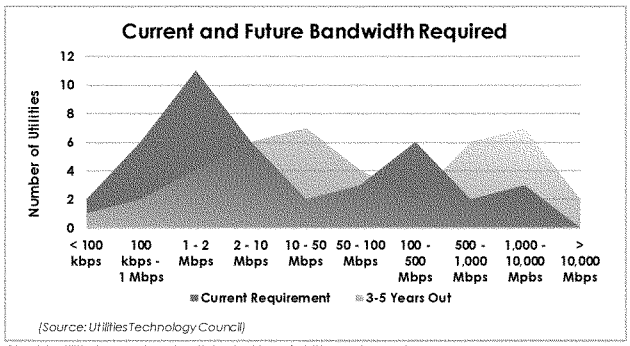


Chart 8 Utilities' current and anticipated bandwidth requirements

Chart 8 shows utilities' current bandwidth requirements and their anticipated requirements in 3-5 years. The solid blue area represents current requirements, while the pastel red overlay represents the anticipated bandwidth needed in 3-5 years.

The right-facing motion from the blue to red chart areas shows a growth in bandwidth requirements over the near-term. Whereas the two current peaks occur at 1-2 megabits per second (Mbps) and 100-500 Mbps, the peaks in the future bandwidth demand occur at 10-50 Mbps and 1,000 – 10,000 Mbps. Both cases represent a tenfold increase in bandwidth requirement over the next 3-5 years.

As mentioned earlier, grid modernization and streaming video drive this medium-term growth in bandwidth consumption. Future bandwidth requirements are based upon current grid modernization projects, typically having a 5-10-year outlook. The bandwidth projections can be considered stable. Thus, a private network with a known capital and operational expenditure may present a stronger financial case than carrier-provided services. Utilities will also consider exceptional operations such as disaster recovery when debating private versus carrier services. Utilities may still need telecommunications carrier services for outlier use cases.

 © 2017 Utilities Technology Council

Network Composition: Current and Medium Term

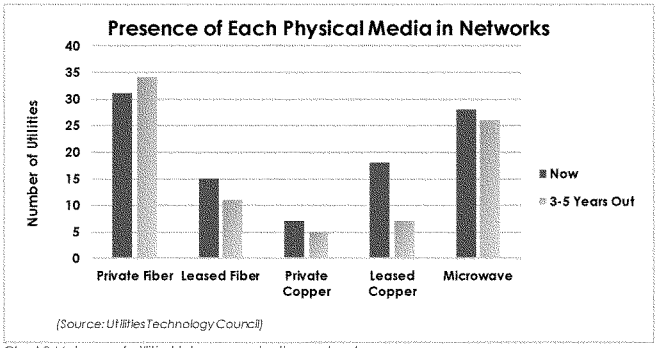


Chart 9 Make-up of utilities' telecommunications networks

This chart combines the different physical media present in utilities' telecommunications now, and those utilities' forecasts of what their networks will look like in 3-5 years. Of particular note is the move away from leased copper over the medium term. That migration results from grid modernization, which is built upon software that communicates using the Internet Protocol (IP), and which requires bandwidth that fiber and microwave can deliver more efficiently.

Microwave and fiber usage appears stable, although there is a slight move from leased to private fiber. Importantly, utilities will continue to add capacity into their wireline and wireless network as demands increase. Private utility networks are here to stay for the long-term.

Respondents also had the option to select satellite telecommunications, but the responses were negligible. Satellite can serve some niche requirements such as short-term solutions until a permanent link can be built, or reaching extremely remote and geographically isolated locations. However, geostationary satellites are at too high an altitude (22,000 miles) to meet the latency requirements of protective relays, which typically require a response within 4 milliseconds.

© 2017 Utilities Technology Council

Fiber and Microwave Are the Dominant Network Media

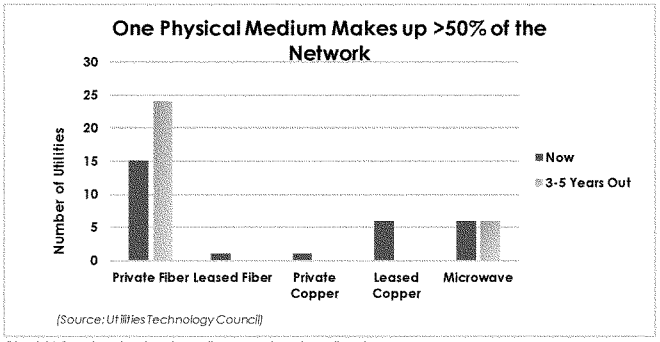


Chart 10 Dominant network media, current and medium term

Chart 10 is a derivative of the chart on the previous page. This chart shows only those utilities where a single physical medium constitutes more than half of their telecommunications capacity. This chart shows more dramatically the move away from copper wire telecommunications, all of it in the direction of private fiber. (Note that the two microwave bars are identical).

Implied in this chart is a substantial capital expenditure for utilities, as they decommission copper wire and replace it with fiber – either Optical Ground Wire (OPGW) or All-Dielectric Self-Supporting (ADSS) cable. Regardless of OPGW or ADSS, UTC members have anecdotally mentioned installation expenses exceeding $100,000 per mile for fiber.

Microwave telecommunications will remain as critical to utilities as they are now. The need for wireless telecommunications with mitigated interference or other operational risk will remain constant, possibly increasing as wireless communications transmit more of the critical reliability data mentioned earlier in this report.

© 2017 Utilities Technology Council

Utilities Mainly Share Networks with Other Utilities

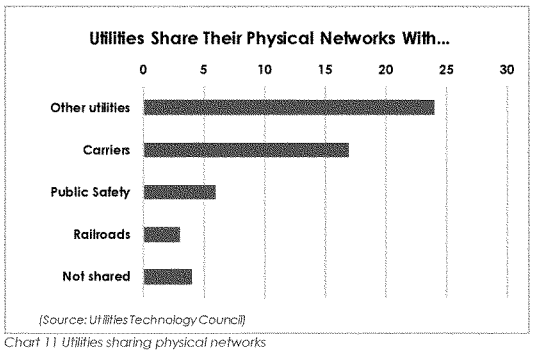


Chart 11 Utilities sharing physical networks

Some utilities have a separate line of business in which they lease unused telecommunications capacity to third parties. This is usually fiber, not wireless telecommunications. As the chart shows, that arrangement is most likely to be made with another utility, although a substantial number of responding utilities also lease unused capacity to carriers.

The overwhelming trend in the responses is that for utilities that do lease unused capacity, they do so to multiple third parties. Most often, a utility that shares its physical network with carriers is also sharing it with other utilities.

Conversely, some utilities steadfastly refuse to lease unused telecommunications capacity. A frequent reason provided is, "That is not our line of business. We are an electricity company."

© 2017 Utilities Technology Council

Licensed vs. Unlicensed Frequency Usage

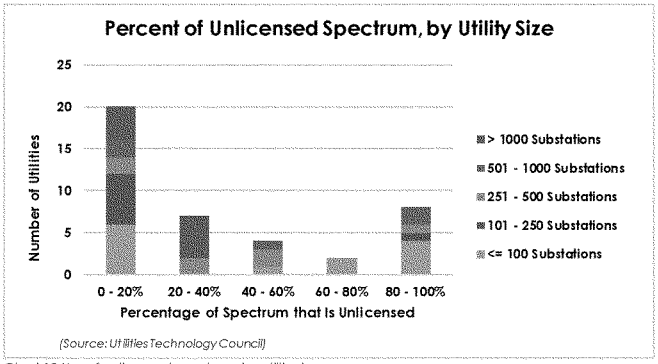


Chart 12 Use of unlicensed spectrum, by utility size

Unlicensed spectrum is freely accessible to utilities, and they must adhere to Federal Communications Commission (FCC) requirements to not cause harmful interference and to transmit at one watt or less. Licensed spectrum is not restricted to low-watt transmission and the FCC actively polices interference. Licensed spectrum, which requires a fee for access, limits the number of users and offers clearer data transmission over greater distances. Chart 12 shows that utilities of all sizes prefer licensed spectrum. Additionally:

- Half of the responding utilities stated that 80% or more of their wireless telecommunications networks use licensed spectrum.
- One-fourth of the utilities said that licensed spectrum accounts for 95% or more of their wireless telecommunications networks.

Life in the unlicensed spectrum can be an adventure. As one UTC member utility responded, "I've lost my frequency three times in 30 years." Each time this utility was forced to move the affected telecommunications to a different frequency range. Different ranges have different propagation characteristics, which in the worst case could require re-engineering microwave paths, building additional towers, and acquiring new radios that work in the new spectrum.

Utilities Rarely Outsource Network Ownership

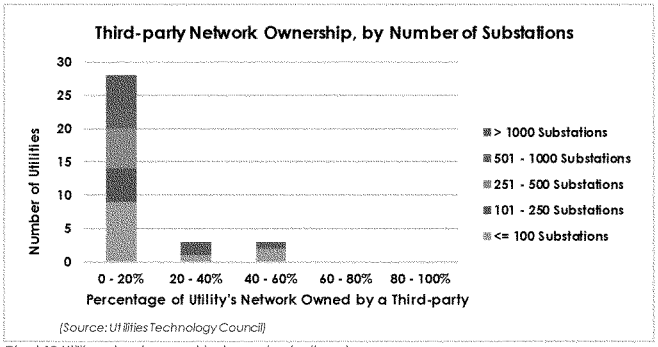


Chart 13 Utility network ownership, by service territory size

This chart shows categorically that utilities do not favor third-party ownership of their telecommunications networks. Interestingly, only the smallest and largest utilities reported any more than 20% of third-party network ownership. Situated at both ends of the spectrum, large and small utilities may be outliers for different reasons and each may have unique reasons for increased third-party ownership.

In the case of large utilities, this may be due to large service areas, as discussed earlier, where some extremely remote sites are best reached with someone else's existing network.

The overriding conclusion from this chart is that utilities prefer to own and operate their own telecommunications networks. Two-thirds of the utilities responded that they own 80% or more of their networks; only one utility reported as low as 40% ownership.

© 2017 Utilities Technology Council

Utilities Rarely Outsource Network Monitoring

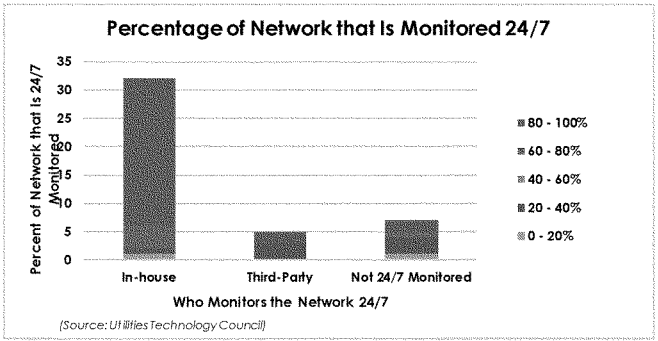


Chart 14 Utility network monitoring

Chart 14 shows that utilities by and large perform their own telecommunications network monitoring. Only two utilities reported that their network is 100% monitored by a third-party.

The vast majority of utilities monitor all of their network in-house. Unlike many other trends in this report, size of utility was a not a factor in whether or not the network is monitored in-house.

Combined with the previous slide's indication that utilities are far more likely to own their own network than to outsource it, the conclusion is that utilities have been able to cost-justify both building and operating their networks in-house. There is additionally a feeling of greater control with in-house ownership and operation – recall the critical energy reliability capabilities supported by these networks.

© 2017 Utilities Technology Council

Carriers Do Not Adequately Prioritize Recovery of Utility Telecoms

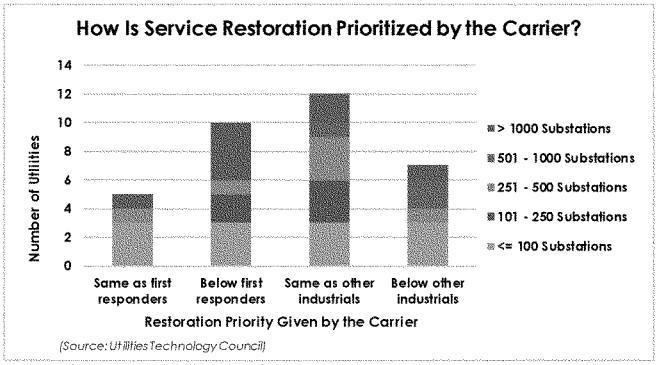


Chart 15 Utility service restoration priority by carriers

Perhaps the most disturbing information from our survey, this chart shows that carriers do not highly prioritize restoration of cellular and other services to utilities. This is ironic given that carriers are highly dependent upon reliable electricity supply for their operations. Especially during disaster recoveries such as after hurricanes, energy and telecommunications must operate in a symbiotic relationship. Each needs the other.

This chart shows a contributing factor to utilities' preference to own and operate their own networks, as shown on the previous two pages: carriers' inability to prioritize service restoration increases the risk that critical telecommunications may be not be available when they are most needed.

Lack of reliable telecommunications impedes a utility's ability to perform disaster recovery. Without reliable data it is difficult to understand the condition of the grid and which facilities need attention first. Aerial surveillance mitigates a lack of telecommunications to some degree. In some cases, lack of visibility into the grid status can lead to increased personnel safety risk.

© 2017 Utilities Technology Council

Lead Time to Enable New Services

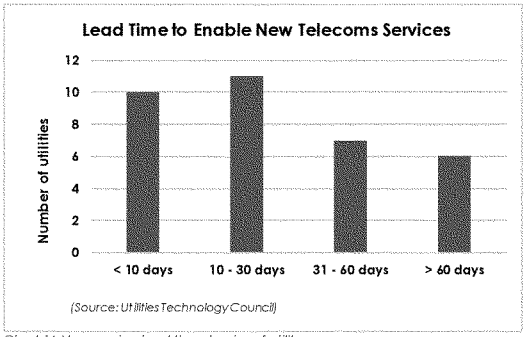


Chart 16 New service lead time, by size of utility

In this chart, the leftmost bar is the place to be: short lead time to enable new services. Curiously, there is little differentiation of lead time by size of utility. Although the survey responses do not provide data to explain this riddle, there are several scenarios to consider:

- Large utilities can have a short lead time because they can afford to outsource service enablement, with short lead times mandated in the service agreements.
- Conversely, large utilities, like nearly all large organizations, are likely to have more sophisticated processes for new service enablement, which can reduce risks but also increase the number of approvals necessary and the elapsed time needed to navigate those more sophisticated processes.
- By comparison, small utilities are on the opposite side of both those scenarios. They may be less able to outsource new services, or to demand the same lead times that large utilities received. But they may also have less process overhead, with fewer decision gates and approvals needed, which allows them to move more quickly.

© 2017 Utilities Technology Council

The CHAIRMAN. Thank you, Ms. Ditto.
Mr. Galloway, welcome to the Committee.

STATEMENT OF THOMAS J. GALLOWAY, SR., PRESIDENT AND CEO, NORTH AMERICAN TRANSMISSION FORUM

Mr. GALLOWAY. Chair Murkowski, Ranking Member Cantwell and members of the Committee, thank you for inviting me to testify today.

My name is Tom Galloway, and I'm the CEO of the North American Transmission Forum. The Forum is a voluntary membership of transmission owners and operators with a mission to promote excellence in reliable, secure and resilient operation of North America's electric transmission system. We believe that timely sharing of information among Forum members, such as best practices and operating experience, is key to advancing performance beyond mandatory levels. Our 89 members of various types and sizes, together, represent over 80 percent of the peak electrical load in the U.S. and Canada.

I'll focus primarily on resiliency which deals with high-impact, low-frequency events, sometimes called Black Sky events, that could cause a system-wide outage. Black Sky events require cross-sector collaboration, alignment of restoration priorities, mutual aid and robust communications. Given the importance of these topics, we've made several of our internal documents public and I've attached those as part of my written testimony, including a summary of backup capabilities and how to cope with the loss of some standard operator tools.

I'll cover five main points in my oral testimony.

First, the restoration varies extensively based on the outage specifics, including the scope, duration, equipment damage and access to restoration areas. There are many commonalities to be sure, but no two outages are exactly alike. And the industry needs and has well thought out, prioritized, and tested restoration plans, but they also need agile decision-making that can navigate the complex and unpresuming circumstances. Blackstart resources are rarely used but are critical when portions of the system cannot be reenergized by connecting to adjacent energized systems.

Point two, severe weather has caused the majority of recent significant events. And while those impacts have been profound, such as those being observed in the Hurricane Michael currently, there are several positives. The industry has applied lessons learned and improved comparatively in a number of cases. So, for example, Florida Power implemented a number of significant upgrades following hurricanes in the 2004–2005 season. As a result, their performance was demonstratively better in 2017 with customer outage times essentially cut in half from a much more severe hurricane Irma.

Point number three, the scope and pace of industry change is unprecedented. And while some of these changes add significant reliability and economic benefits, they do add complexity to both operate the system and restore from outages. These changes include generation of fuel mix, increased use of interconnected digital technologies at both physical and cyber threats. Areas of continued focus related to these topics include interoperability issues between

sectors and the security of an increasingly interconnected digital grid.

Point four, there are a number of beneficial no-regrets actions that are underway having to do with equipment spares, testing, mutual aid and drills. For example, Con Edison has developed, tested and deployed resiliency transformers which are smaller modular devices that could be installed quickly in a variety of system locations if their primarily used transformers are damaged for some reason. Likewise, Con Ed is testing feasibility of blackstart recovery in the midst of an ongoing cyberattack.

The mutual aid process in the industry is well established and evolving. In Hurricane Irma, that I mentioned earlier, Florida Power imported over 11,000 linemen from across the company—from across the country as far away as California—to help aid in that restoration, and mutual aid efforts are now being evolved to include specialized expertise such as cybersecurity.

The industry is also conducting increasingly sophisticated drills such as last week's Southern California Edison conducted their fifth annual resilient grid exercise. This simulated a combined physical and cyber attack that impacted Southern California Edison and some of their adjacent systems. They also introduced losses of normal communication and some of the normal operative tools to further complicate the scenarios. The after-action discussions were very robust, including representation of cross-sector and governmental representatives that focused on the need to align our priorities and effective educations.

I'll summarize very quickly. In terms of going forward, I believe that industry and regulators should align on resiliency priorities, focus on no-regrets actions that are applicable to multiple hazards that promote recovery for prudent investments. And I think there's a strong focus needed on communications capabilities, referred to by Ms. Ditto, both in terms of technologies, redundancy, diversity and also communication protocols.

Thank you for the opportunity.

[The prepared statement of Mr. Galloway follows:]

North American Transmission FORUM

Community Confidentiality Candor Commitment

Written Testimony
Hearing of the U.S. Senate Energy and Natural Resources Committee
October 11, 2018

Thomas J. Galloway Sr.
NATF President and CEO

The purpose of the hearing is to examine black-start, which is the process for returning energy to the power grid after a system-wide blackout, and other system restoration plans in the electric utility industry.

I. Background

Chair Murkowski, Ranking Member Cantwell, and members of the committee – thank you for inviting me to testify on black-start and other restoration considerations in the electric utility industry. My name is Thomas (Tom) J. Galloway and I am the president and CEO of the North American Transmission Forum (NATF).

The NATF is a voluntary membership of transmission owners and operators, formed in response to the August 2003 blackout, with a mission to *promote excellence* in the reliable, secure, and resilient operation of North America's electric transmission system. The NATF was modelled after the Institute of Nuclear Power Operations (INPO), which has a analogous mission for the commerical nuclear power industry. The NATF's 89 members include investor-owned, municipal, cooperative, U.S. federal, and Canadian provincial utilities, as well as ISOs and RTOs, and together represent over 80% of the peak electrical load in the U.S. and Canada. The NATF is built on the principle that timely sharing of detailed information—best practices, operating experience, lessons learned, and areas for improvement—among its members is key to advancing transmission system performance beyond mandatory levels, especially during times of rapid industry change[1].

Bulk power system reliability and resiliency are closely related characteristics with some important distinctions. In the NATF's context, reliability expresses how seldom portions of the system "fail" or become undependable due to traditional impacts like equipment malfunctions and tree contacts. These impacts cause outages of varying frequency and duration that can disrupt end users. In the most extreme cases, such as the August 2003 blackout, the compounding of several "traditional" impacts can result in cascading outages that affect a large geographic area for days or even weeks. Resiliency involves severe, infrequent, and often non-traditional impacts. These high-impact, low-frequency (HILF) impacts—also called "gray sky" and "black sky" days—include threats such as extreme natural events or a postulated coordinated cyber-physical attack, respectively. In the most extreme cases, gray sky or black sky events are presumed to extend weeks or longer.

Mandatory reliability standards play a key role in reliability and resiliency, but other more-agile solutions are becoming ever more important given the pace of industry change and evolving threats. Accordingly, the NATF has placed increasing focus on resiliency in recent years. The NATF's resiliency approach considers that a severe impact, however unlikely, could occur; therefore, it necessitates advanced planning, hardening, processes to "operate through" the impact, and restoration strategies based on various considerations, including geographic scope, types of equipment involved/damaged, expected duration, cross-sector implications, and causes. Since severe-impact events could result in long-duration outages, alignment on restoration priorities, cross-sector collaboration, mutual aid, and robust communications are critical.

[1] For more information, please visit www.natf.net

Open Distribution
Copyright © 2018 North American Transmission Forum. Not for sale or commercial use. All rights reserved.

In addition to confidential work, the NATF has shared select resiliency documents publicly, including ones focusing on the topic of supplement operating strategies (SOS) that deal with a broad loss of important operator tools during these types of events. Further, the NATF has engaged with the Department of Energy (DOE) and others on a standardized framework for response to a declared Grid Security Emergency (GSE).

II. Key Points

My testimony will cover five main points as listed below. In addition, I've included applicable attachments.

1. ***Restoration plans, priorities, and performance vary greatly based on the outage***
   Outage factors, such as geographic scope, duration, and involved elements and equipment; conditions, including the ability to move needed resources into affected areas; and specific cause(s) all greatly influence restoration. Black-start resources are rarely used but critical when portions of the system cannot be re-energized using an interconnection with adjacent, energized systems.

2. ***Natural events (severe weather) have caused the majority of recent significant outages***
   Weather influenced 9 of 10 of the most severe outages from 2008–2016. And that pattern has continued with hurricanes Irma, Maria, and (recently) Florence. While those impacts have been profound, lessons learned have been applied and system robustness has increased; over time, restoration performance has improved comparatively in many instances. Many of these enhancements support improved resilience for other, potentially more-severe non-weather-related events.

3. ***Bulk power system changes underway increase operational and restoration complexity***
   The scope and pace of industry change is unprecedented, including new dynamics in generation fuel mix, new technology, regulation, economics, and public-policy priorities. These changes provide various benefits but, in some cases, increase the complexity of both operating the bulk power system and restoring the system from outages.

4. ***Beneficial "no regrets" actions are being implemented***
   Significant efforts are underway to educate on threats, harden the bulk power system, ensure adequacy of key spares, augment mutual aid, enhance restoration plans, conduct comprehensive drills and exercises, and increase coordination—both cross-sector (e.g., gas, water) and with governmental partners (FERC, the DOE, etc.). The NATF is promoting an "all hazards" approach, with focus on actions that provide benefit under various scenarios.

5. ***Going-forward emphasis***
   Rather than create new or revised standards focused on individual resiliency hazards, FERC and the ERO should emphasize "no regrets" activities applicable to a range of resiliency hazards. The ERO should increase work with regulated entities and state regulators to align on system resiliency priorities and promote recovery for prudent investments (e.g., diverse and redundant black-start). The current grid command and control hierarchy is very effective and will be so in black sky events if communication capabilities are sufficient. Added focus on strengthening communications—technology, redundancy, diversity, and protocols—is essential.

III. Point 1: Restoration plans and priorities vary based on the outage

Outage factors, such as geographic scope, duration, and involved elements and equipment; conditions, including the ability to move needed resources into affected areas; and specific cause(s) all greatly influence restoration. Black-start resources are rarely used but critical when portions of the system cannot be re-energized using an interconnection with adjacent, energized systems.

Geographic scope

Generally, a broader geographic outage scope results in a more-difficult restoration and greater likelihood of reliance on black-start resources. In most outages, adjacent energized systems can be relied on to help restore power to the blacked-out sections. In addition, most electric utilities have a prioritized list of customers for restoration based on the local criticality of those loads, contractual obligations, etc. As the scope extends to multiple companies or regions, however, the likelihood increases that restoration priorities will not fully align. Reliability Coordinators and others with a wide-area view effectively assist in prioritizing restoration, but prioritization challenges further increase when scope exceeds available restoration resources (personnel and equipment) or other sectors (e.g., natural gas, communications, etc.) are involved. For example, electrical service to assets needed for generation fuel delivery may take on a higher priority in certain restoration scenarios.

Duration

Outage restoration from most traditional impacts is typically measured in minutes, hours, or occasionally days. As the expected outage duration extends to many days to perhaps weeks, restoration priorities must be re-evaluated and revised. Outages of very significant duration can be further complicated by evacuation of residents (rather than sheltering in place) and prohibiting access to affected areas by other than essential personnel (restoration crews, first responders, etc.).

Specific location – including the ability to move needed restoration resources into affected areas

Outage location and local conditions directly influence the restoration. Factors such as flooding or extreme cold and the ability to physically move restoration resources into the area influence restoration priorities and plans. As an example, during Hurricane Florence, significant flooding impeded restoration efforts. Similarly, restoration activities in Puerto Rico following Hurricane Maria were significantly complicated by the logistical challenges associated with moving resotration personnel and equipment to the island.

Criticality of Loads

Certain loads are by definition more critical, such as prompt restoration of offsite power to nuclear power plants. Further, if the outage impacts defense-critical installations, restoration priorities from a national security perspective may compete with local priorities, such as restoration to hospitals. Outages impacting those types of critical loads greatly influence restoration priorities.

Involved elements and equipment

Most outages from traditional impacts are distribution-centric. Distribution circuits are at lower voltage, provide power to a smaller subset of customer loads, and typically are not cost-effective to harden to the same extent as transmission level assets.

Some outages are generation-centric—such as the January 2014 "Polar Vortex" event (see NERC review – September 2014)—and require different restoration approaches.

Outages, even extremely large ones, can occur with limited equipment damage. For instance, the August 2003 Northeast blackout that interrupted power to about 40 million people was precipitated by vegetation contacts resulting in a cascading outage. Weaknesses in operator tools used to monitor the system delayed intervention to curtail the event. However, there was limited equipment damaged during the event. And while some customers were without power for extended periods, restoration to the majority of the system was accomplished in a few days.

Outage restoration is complicated in cases where unique, important, or significant amounts of equipment are damaged. To reduce that impact, the industry has placed considerable focus ensuring adequate spares and alternate approaches—such as pooled resources and sharing—for significant, long-lead-time equipment such as large power transformers.

Specific causes) impact restoration

In addition to those involving significant equipment damage, outages from malicious acts, such as a coordinated cyber-attack, could additionally impact restoration priorities and performance. In such cases, tools that operators use to monitor the system could also be impacted, limiting situational awareness and impeding decision-making. Further, outages involving a physical attack on electric system assets could impede restoration activities given the needed steps to ensure safety of restoration personnel.

IV. Point 2: Natural events caused the majority of recent significant outages

The top-ranked outage listed in NERC's "2017 State of Reliability Report," based on severity risk index, was the September 2011 "Southwest Blackout." This event was caused by weaknesses in two broad areas—operations planning and real-time situational awareness. However, weather influenced 9 of 10 of the most severe outages from 2008-2016. And that pattern has continued with hurricanes Harvey, Irma, Maria, and (most recently) Florence. While those impacts have at times been profound, lessons learned have been applied and, over time, restoration performance has improved comparatively in many instances.

For example, following hurricanes in 2004 and 2005, Florida Power & Light (FPL) implemented significant system upgrades, including strengthening over 800 lines that supply critical infrastructure, moving underground or otherwise hardening about half of its main power lines, upgrading over 200 substations in flood-prone areas with specific mitigations, installing over 80,000 intelligent devices (automatic feeders, etc.), implementing mobile command centers, and increasing drone use for damage assessment. As a result of these improvements, FPL performance during 2017's Hurricane Irma (a much more severe storm than those seen in 2004–2005) was demonstrably better, with average customer outage times essentially cut in half (2.3 days versus 5.4 days). What is particularly significant is that while these system upgrades improved performance for the targeted hazard (hurricanes), they were in many cases "no regrets" actions that also likely provided collateral resiliency benefits across a number of other credible hazards.

Similarly, Consolidated Edison implemented a number of lessons learned from benchmarking Hurricane Katrina in New Orleans and as a direct result of Hurricane Sandy. These include a defense-in-depth strategy

for important substations, including the use of more-conservative flood design bases, more moats, higher walls, dewatering capability, improved remote-station monitoring feeds aggregated to centralized locations, and added protection for specialized or high-importance equipment.

Hurricane Harvey, which impacted the Houston area was more a "water event" than a "wind event." This necessitated restoration and recovery techniques never used before in the that area. One key finding from these events was the importance of deploying drones as an effective way to identify field conditions and required restoration activities.

V. Point 3: Bulk power system changes underway increase complexity

The scope and pace of electric industry change is unprecedented, new dynamics in generation fuel mix, technology, regulation, economics, and public-policy priorities. These changes provide various benefits but, in some cases, increase the complexity of both operating the bulk power system and restoring from outages.

Generation fuel mix

Solar, wind, and natural gas generation are increasing while nuclear power and coal generation are decreasing. These changes are the result of factors including economics and public-policy priorities. From an electrical grid operation perspective, the changes introduce several new variables. For example, net loss of large base-load generation that employs a large rotating mass reduces system inertia; therefore, electrical frequency can change more rapidly during a transient and thus be more difficult to control. Solar power and wind are also "intermittent" generation resources, which creates challenges maintaining system balance and ensuring adequate reserves. Further, increased solar use has resulted in a corresponding increase in inverters. Several system events have resulted from inverter operating characteristics that were not fully understood.

From a system-restoration perspective, including during the use of black-start, reduced diversity in generation fuel source adds uncertainty. For instance, to the extent that natural gas generation dominates as the fuel source, the grid is potentially more susceptible to outages caused by interruption of that nearly "just-in-time" fuel supply. Grid operators are now performing exhaustive analyses to better understand electrical system sensitivity to the changing fuel mix along with appropriate compensatory actions.

New technology

Extensive use of new technology is revolutionizing how the grid operates. To name but a few, these include utility scale photo-voltaic (solar) generation resources, increased use of large-scale battery storage, prevalence of digital protection system devices (in favor of electro-mechanical relays), micro-grids, use of unmanned aerial systems (drones) for damage assessment, addition of smart meters for automatically reporting of power outages to control centers, and more-sophisticated grid modeling and situational awareness tools. These technology advances are allowing the grid to become even more tightly interconnected and offer a broad range of reliability, resiliency, and economic benefits.

However, the extensive use of advanced technology introduces challenges, including new requisite personnel skills (e.g., relay technicians need to be proficient in setting digital equipment and legacy electro-

mechanical equipment), potentially unrecognized operating characteristics or failure modes, and possible susceptibility to cyber-attack via supply chain and other vectors.

Regulatory changes/jurisdiction

The North American Electric Reliability Corporation (NERC) was certified by FERC as the Electric Reliability Organization (ERO). As the ERO, NERC is charged with enforcement of mandatory reliability standards for the bulk electric system. These standards became mandatory and enforceable on June 18, 2007. NERC is also responsible for conducting various assessments related to the bulk power system. Since certification as the ERO, NERC has matured significantly, with increasing focus on proactive risk identification.

While NERC, under oversight by FERC, is responsible for bulk electric system regulation, individual states have jurisdiction over the lower-voltage electrical distribution within their respective geographic areas. Additionally, under the FAST Act, the DOE was granted authority to issue orders to grid operators upon a presidential declaration of a Grid Security Emergency (GSE). GSEs are characterized as occurrence or imminent danger of one or more of four specific types: geomagnetic disturbance (GMD), electro-magnetic pulse (EMP), physical attack, or cyber-attack. Varying jurisdictions and authorities introduce increased complexity regarding alignment of priorities. And compliance obligations, without commensurate economic incentive, is a possible contributor to reduction in dedicated black-start resources.

Security (Physical and Cyber)

Physical Security

In April 2013, gunmen, using rifles, conducted a sophisticated attack on an important transmission substation. During this attack, 17 electrical transformers were severely damaged at a cost to repair of several million dollars. Prior to the attack, a series of fiber-optic telecommunications cables were cut in an apparent attempt to delay detection of, and response to, the attack. There were no injuries and the event had little direct impact on reliability of the electrical system. However, the electrical industry responded to this attack as a hallmark event, and accelerated efforts underway to bolster resiliency and security. These included fast-track development of a new NERC reliability standard (CIP-014) regarding determination and assessment of critical substations.

Cyber Security

Protecting the electrical grid from a variety of cyber threats is a top industry priority. Cyber security threats, as evidenced by the 2015 attack on the Ukrainian electrical grid, can be impactful. And the threats are becoming increasingly sophisticated. In an attempt to keep pace, NERC leadership has placed cyber security as a top priority and is currently on version 5 or greater for the associated Critical Infrastructure Protection (CIP) standards. In addition to evolving security threats, such as vendor supply chain vulnerabilities and increased use of cloud-based storage, other challenges include industry burden complying with changing mandatory standards, limited access to real-time threat information, and finite (and mobile) workforce cyber security skills. In my opinion, one of the most pressing concerns involves the nexus between increased connectivity of grid digital assets coincident with increasing cyber threats.

VI. Point 4: Beneficial (no-regrets) actions are being taken

Significant industry efforts have been taken and are underway to preserve high levels of grid reliability and resiliency and improve restoration from broad-scope outages. These actions include educating the industry and regulators on resiliency threats, hardening the bulk power system, ensuring adequacy of key spares, augmenting mutual aid, enhancing restoration planning, conducting comprehensive drills and exercises, and increasing coordination—both cross-sector (e.g. gas, water) and with governmental partners (FERC, the DOE, etc.).

Education

Following the April 2013 substation attack, the NATF and the Electric Power Research Institute (EPRI) began jointly conducting resiliency summits to help align industry efforts and advance performance. The NATF and EPRI are focused on an "all hazards" approach with an emphasis on implementation of "no regrets" actions. To date, over 10 summits have been completed with attendance typically consisting of greater than 100 industry experts, regulators, and representatives from government. The initial set of summits focused on highlighting the importance of resiliency, clarifying similarities and differences between reliability and resiliency, and identifying various threats. More recent summits have focused heavily on restoration and cross-sector coordination.

System Hardening

The industry has placed extensive effort on hardening transmission systems from known, relevant hazards such as hurricanes and floods. As awareness of and sensitivity to non-traditional resiliency threats has grown, the industry has moved forward with associated hardening on several fronts. These actions include amplifying guidance on how to determine "critical substations," workshops and best-practice documents specific to main control center and substation design and construction from a physical security perspective, EPRI analyses of the consequences of an EMP-event to the electric grid, and implementation by some companies of shielding protection of various key assets from the effects of an EMP. In addition to hardening assets, like main control centers and key substations, the industry has begun improving system models to identify and, where possible, reduce the risk of key assets by ensuring added redundancy and dispersing key functions. Hardening of electric grid systems and components in these ways does not preclude a resiliency impact but helps limit the scope and severity of the casualty, thereby allowing for more timely restoration.

Adequacy of key spare parts and innovative alternatives

The industry's Spare Transformer Equipment Program (STEP) program strengthens the ability to restore the transmission system more quickly in the event of a terrorist attack. STEP is a coordinated approach to increase the spare transformer inventory and streamline transferring those transformers to affected companies in the event of a transmission outage caused by a terrorist attack. Under STEP, each participating company is required to maintain and, if necessary, acquire a specific number of transformers. STEP requires each participating company to sell its spare transformers to any other participating company that suffers a "triggering event," defined as an act of terrorism that destroys or disables one or more substations and results in the declared state of emergency. Any investor-owned, government-owned, or rural electric cooperative electric company in the United States or Canada may participate.

In addition to STEP, the SpareConnect program provides an additional mechanism for bulk power system asset owners and operators to network with others concerning the possible sharing of other selected key equipment. SpareConnect establishes a confidential, unified platform for the entire electric industry to communicate equipment needs in the event of an emergency or other non-routine failure.

Large power transformers are expensive, take a long time to build, and are very difficult to transport. To augment STEP, SpareConnect, and other spare parts approaches, Con Edison and others have developed and deployed "recovery" or "resiliency" transformers. These smaller, modular, and lighter devices are relatively easy to transport and can be quickly placed in service at a variety of key system locations. In January 2017, Con Edison demonstrated a successful installation in less than three days in response to a mock incident. While they do not have the same design lifetime as standard transformers, these recovery transformers could serve as a critical bridge to restore the system while fully pedigreed devices are being obtained. Similar innovative approaches have been developed for other key equipment such as control houses.

Augmented mutual aid

Mutual aid is key to successful restoration from a broad system outage. The electric industry uses this approach extensively to surge added resources (lineman, equipment) into an affected area to help in outage restoration. Collaboration and reciprocity under these mutual aid approaches have been highly successful and have continue to evolve. In addition to lineman resources, the mutual aid now sometimes consists of associated management teams from the supplying company to help manage restoration in pre-determined areas under the general oversight of the host company. Based on lessons learned from Hurricane Sandy, the industry developed a new governance structure termed a "National Response Event" to help prioritize and assign larger sets of mutual aid resources from even-more-distant locations. A recent area of focus involves developing an equivalent mutual aid capability for specialized skill sets, such as cyber security personnel or protection system technicians that could prospectively be shared in the wake of a relevant event.

Enhanced restoration plans

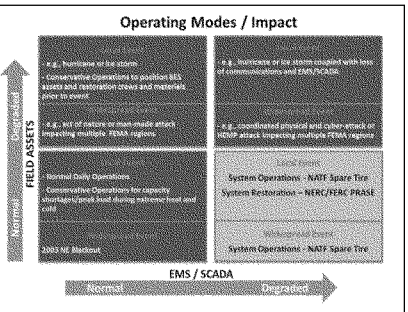
One specific area of "no regrets" action involves enhancements to restoration plans. Several NATF-EPRI resiliency summits have featured presentations and stressed emulation of National Incident Management System (NIMS) / Incident Command Structure (ICS), which encourages a whole community perspective to restoration and a common command and control hierarchy, respectively. Other summits have featured presenters from other industry sectors (water, gas, communications, etc.) to help clarify interdependencies that need to be factored into restoration priorities. Further, FERC and NERC have together conducted two different sets of inquiries to understand industry readiness to restore from system events as required by certain mandatory standards. Lastly, the NATF has commenced two separate restoration related projects—Supplemental Operating Strategies (SOS) and a report to the DOE on GSEs.

NATF Supplemental Operating Strategies

The Supplemental Operating Strategies (SOS) effort presumes a broad loss of some key operator tools (EMS/SCADA) used to monitor and control the electrical system due to cyber-attack or other impact. The SOS project identified a rank-order set (shown below) of key capabilities operators would need in order to manually operate or restore the system given an EMS/SCADA loss (shown below) with some proposed

compensatory actions. Future SOS project phases will consider coincident degradation of field assets, such as key substations.

Key Capabilities / *Priority Rank Order*
1. External Voice Communications
2. Internal Voice Communications
3. Area Control Error Calculation
4. Frequency Telemetry
5. Transmission System Monitoring and Control
6. Generation Dispatch and Automatic Generation Control
7. Personnel Deployment (Human Remote Terminal Unit)
8. State Estimation / Real-Time Contingency Analysis
9. Interchange Scheduling
10. Off-line Power Flow Analysis
11. Load and Wind Forecasting



NATF report to the DOE on GSEs

Section 215A of the Federal Power Act, added via amendment by section 61003 of Public Law 114-94 (the Fixing America's Surface Transportation Act or "FAST Act"), gives the Secretary of Energy certain authorities to issue an emergency order following the president's written declaration of a "grid security emergency" (GSE) as defined in the statute:

The term 'grid security emergency' means the occurrence or imminent danger of—(A). . . a malicious act using electronic communication or an electromagnetic pulse, or a geomagnetic storm event . . . and . . . disruption of the operation of such devices or networks, with significant adverse effects on the reliability of critical electric infrastructure or of defense critical electric infrastructure, as a result of such act or event; or (B) . . . a direct physical attack on critical electric infrastructure or on defense critical electric infrastructure; and . . . significant adverse effects on the reliability of critical electric infrastructure or of defense critical electric infrastructure as a result of such physical attack.

Because of the specialized knowledge and the wide range of designs and practices inherent in the companies that own and operate the bulk power system, the NATF has convened a GSE Team to offer recommendations on the following:

I. Communication between the U.S. Department of Energy (DOE) and the electricity subsector after the declaration of a GSE

II. Suggested criteria for declaring a GSE

III. Emergency operations and waivers associated with issuance of a GSE order

The current NATF document addresses prospective communication and waivers for all four types of threats associated with a GSE order—geomagnetic disturbance (GMD), electromagnetic pulse (EMP), cyber security,

and physical security. It also provides suggested criteria for declaring a GMD GSE. Suggested criteria for the other three emergencies (physical, cyber, and EMP) will be addressed in subsequent updates to this document.

Increasingly comprehensive drills and exercises

Electric companies routinely drill on and refine their restoration plans. Several NATF members have greatly increased the scope and complexity of these drills, including enhancements such as cross-sector coordination and assuming a loss of EMS/SCADA to test readiness for that situation.

SCE Resilient Grid V

One recent positive example is Southern California Edison's "Resilient Grid" exercise conducted on October 4, 2018. This was the fifth such exercise and considered a simulated combined cyber and physical attack that affected multiple assets within SCE and several other neighboring systems resulting in extensive residential customer outages and disabling of two major seaports, with the attendant economic impact. The drill emphasized needed cross-sector coordination as well as timely/measured updates to the public. To further complicate the drill and test restoration capabilities, SCE presumed a loss of EMS/SCADA (as presumed in NATF SOS documents) and interruptions in normal communications. The after-action roundtable discussed matters of critical interdependencies, cyber-attack liabilities, and the benefits and complexities of declaring such a situation—were it real—as a GSE.

Con Edison work with DARPA / RADICS

Con Edison is working with the Defense Advanced Research Projects Agency (DARPA) on testing of its Rapid Attack, Detection, Isolation, and Characterization Systems (RADICS) program. The objective of this program is to create a testbed and associated exercises to test feasibility of a black-start recovery in the midst of an ongoing cyber-attack. It involves coordination between operational and cyber experts and reviews how tools and technologies perform with limited power and ancillary services.

Another NATF member recently conducted a three-day long exercise that combined a cyber-attack with a natural disaster impacting a major city's critical infrastructure. Ninety exercise players participated overall, including major infrastructure owners from various sectors and local, state, and federal agencies. Exercise objectives were to build capabilities and coordination for enhanced incident response and recovery, and strengthen collaboration across sectors, jurisdictions, and disciplines.

VII. Point 5: Going-forward emphasis

Considering the industry changes and current work underway regarding resiliency, we believe the following would be beneficial:

- FERC, NERC, and the Regions should continue and increase work with regulated entities and state regulators to align on priorities for system hardening and to promote recovery for prudent investments.
- Rather than create new or revised reliability (or resiliency) standards that focus on individual hazards or threats, conduct a comprehensive review of existing relevant standards (such as TPL-001) to determine baseline performance that would improve resiliency regardless of the hazard.
- The current grid command and control hierarchy (Reliability Coordinators, Balancing Authorities, etc.) is very effective and will be so in black sky events if communication capabilities are sufficient. Much of NATF resiliency work has underscored the importance of reliability communications as a key tool to prepare for, operate through, and restore from severe events. Added focus on strengthening communications—technology, redundancy, diversity, protocols—is essential.
- Lastly, resiliency performance improvements can be measured after implementation through traditional metrics (such as FPL's reduction in average customer outage times); however, added measures are likely needed to proactively understand system resiliency and any important gaps. These measures could take the form of a maturity model.

Attachments

Documents related to NATF Supplemental Operating Strategies (SOS)

North American Transmission FORUM

Bulk Electric System Monitoring and Control - An Overview of Backup Capabilities

Disclaimer

This document was created by the North American Transmission Forum (NATF) to facilitate understanding of Bulk Electric System Monitoring and Control Backup Capabilities. NATF reserves the right to make changes to the information contained herein without notice. No liability is assumed for any damages arising directly or indirectly by their use or application. The information provided in this document is provided on an "as is" basis. "North American Transmission Forum" and its associated logo are trademarks of NATF. Other product and brand names may be trademarks of their respective owners. Copyright 2016. All rights reserved. This legend should not be removed from the document

Open Distribution

Copyright © 2016 North American Transmission Forum. Not for sale or commercial use. All rights reserved.

Contents

Bulk Electric System Monitoring and Control - An Overview of Backup Capabilities 13
Contents 14
Introduction and Purpose 15
Background of the Bulk Electric System (BES) 15
Overview of Key Control System Functions 16
Resiliency of Key Operating Infrastructure 16
Operations Control Centers 16
Control Center Infrastructure 16
Defense in Depth for System Operations 17
Business Continuity 18
Conclusion 18

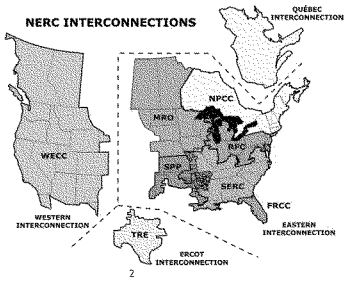
Introduction and Purpose

The Bulk Electric System (BES) is a complex network of electrical generation resources and transmission lines designed and operated to provide continuous and reliable electrical service. A key element in the reliable operation of the BES is the control centers that continuously monitor and control the generation and transmission power flows on the BES. Given the importance of these control centers, their infrastructures, and the tools utilized therein, there are a variety of methods employed to ensure these critical capabilities remain available and operational during both normal and emergency situations.

This document is intended to provide an overview of the key capabilities for the reliable operation of the BES, along with a description of the various approaches used within the industry to ensure redundancy for critical capabilities so that System Operators are able to continuously monitor and control the BES in the event of the loss of the primary control center capabilities.

Background of the Bulk Electric System (BES)

In North America, there are four Interconnections that operate independently of one another in order to provide economic and reliability benefits to all the interconnected entities.



2

- Eastern Interconnection
- Western Interconnection
- Texas Interconnection
- Quebec Interconnection

The nature of the AC interconnected system is such that continuous, diligent coordination within an Interconnect is essential to maintaining reliability. The BES is organized hierarchically, and within the Interconnections, there are one or more Reliability Coordinators (RCs) with authority to preserve reliability within their specific territories. Each RC has one or more Balancing Authorities (BAs), charged with maintaining proper load and generation balance (resulting in preserving system frequency within appropriate bounds), and one or more Transmission Operators (TOPs), charged with maintaining acceptable voltage and line flows. All of these entities work together both in real-time and for future time frames to ensure reliable operation of the BES.

[2] http://www.nerc.com/AboutNERC/keyplayers/Documents/NERC_Interconnections_Color_072512.jpg

Overview of Key Control System Functions

The reliable operation of the BES requires a high degree of coordination between multiple operating entities (RCs, TOPS, BAs, Generator Operators (GOPs), field personnel, etc.) and the assimilation of vast amounts of data. This provides System Operators with the information necessary to maintain situational awareness and to ensure the system remains in a reliable state as loads, transmission configuration, and generation output continuously change. The primary tool used by System Operators is the Energy Management System (EMS). The EMS provides the capability to assimilate and monitor system parameters in real-time, predict their future state and control equipment status and output to ensure system reliability. The EMS also implements Supervisory Control and Data Acquisition (SCADA) for the transmission system, which enables both monitoring and control of the grid.

Key Functions of an EMS/SCADA system can be characterized in five high level categories:

- Status and Control of the Transmission System
- Contingency Analysis of the Transmission System
- Status and Control of Generators
- Management of Generation Reserves
- Energy Accounting

Resiliency of Key Operating Infrastructure

Operations Control Centers

Control centers provide System Operators with the capability to reliably operate the electric grid while also ensuring continued operations should an event render a control center inoperable. In order to ensure functional obligations are maintained during adverse conditions impacting a primary control center, backup control center facilities are in place, with the same functional capabilities of the primary facility, allowing continued operation of the BES. NERC standard EOP-008-1 requires backup control center capabilities for the RC, TOP, and BA functions.

The primary/backup control center configuration design and System Operator functions within a control center vary based on the organization's functional responsibility, the structure of the organization, and the size or configuration of the service area. Similar to the variations of a control center's internal configuration, the procedures for operating a primary and backup control center also varies across the industry. The three typical configurations employed are often referred to as having a "hot/cold", "hot/warm", or "hot/hot" design.

Primary control centers are considered the "hot" facility while the backup control center is generally a "cold" standby facility that can be fully staffed and activated within two hours (per NERC standard EOP-008-1). Typically, the average time from primary to backup facilities is less than one hour away. The operation and maintenance of a tertiary operating facility is not typical within the industry. However, there are some examples of configurations that allow transfer of full or limited capabilities to an alternative facility.

Control Center Infrastructure

In addition to maintaining control center redundancy, many layers of protection for critical control center infrastructure are also employed. These include the following:

1. **Computing Capability and configuration:** Control Center tools are commonly provided via high-availability computing architectures. Energy Management Systems (EMS) and other control center systems are typically configured to provide a redundant pair for each system component for the primary control center plus an additional redundant pair for the Backup control center.
2. **Cyber Protection:** The computing systems for control systems are commonly embedded and logically separated within the larger corporate data networks. This separation enables these networks to benefit from the cyber protections deployed to protect the larger corporate networks, along with the ability to deploy more specific protection for the control network environments. Entities also employ physical security plans and measures to control access to Critical Cyber Assets as defined by the NERC CIP Standards.
3. **Power Supply, HVAC and other facility support infrastructure:** Control centers are designed for continued operation when off-site power from the local utility is unavailable. In many cases there are redundant off-site sources from the local utility along with redundant on-site generation capability. The typical configuration may also include an Uninterruptible Power Supply (UPS) with batteries to provide power to the control center during the transition from the local utility to the on-site generation. Many control centers utilize dedicated and redundant chillers, air handlers, and Computer Room Air Conditioning (CRAC) systems to ensure continued operations during equipment failure or maintenance.
4. **Data Communications:** There are a variety of data sources utilized by EMS and other System Operator tools. Data communication paths for applications are typically composed of a combination of commercial vendor data networks and proprietary private networks to create acceptably redundant communications networks. The private networks may consist of fiber, microwave, or other wireless technology.
5. **Voice Communications:** Voice communications between field personnel, TOPs, BAs, GOPs, and RCs are critical in managing BES reliability. Control centers employ layers of redundancy to minimize the probability of loss of voice communications systems. These various forms of communications include: corporate networks, direct commercial landline service, commercial cellular, and satellite phones. In some cases, entities also have access to proprietary radio, cellular, instant messaging or video link communication tools. All RCs and many TOP/TOs also have access to a NERC-managed messaging system (RCIS) for communication with neighboring control centers. In addition, all RCs have access to a NERC-managed dedicated phone line (NERC Hotline) for communication between RCs.
6. **Physical Security:** In addition to the Cyber Asset physical security measures mentioned above, the most critical control centers, as defined by NERC standard CIP-014-2 requirements, have undergone stringent threat and vulnerability assessments along with a review of their respective physical security plans. These plans are also required to be reviewed and endorsed by independent third parties. Control centers, at a minimum, generally employ on-site security and multiple check points with controlled access to control rooms and data rooms.

Defense in Depth for System Operations

As noted, significant effort is made to protect essential infrastructure and capabilities for the reliable operation of the BES. Regardless, there will ultimately be times for which extreme events may introduce brief moments of degraded operating capability for a particular set of tools or location. Fortunately, in addition to an entity's primary and backup systems, System Operators have coordination plans and

capabilities in place that allow them to coordinate operations within and across organizational boundaries. This "defense in depth" principle helps to maintain sufficient operating capability to ensure a reliable BES during even the most severe of operating conditions.

For instance, RC system capabilities will cover the entire host RC region along with modeling some (or all) of their neighboring RC systems (which may include portions of multiple TOP systems). This overlap of RC system visibility (host RC, host TOP, and neighboring RC and TOP areas) provides System Operators with multiple layers of redundancy necessary to maintain situational awareness and for coordinated system operations. Likewise, protocols for communication are included in critical operating procedures for both normal and abnormal system operations. Effective coordinated system operations requires robust and redundant internal and external communication capabilities, which are generally designed to include direct phone calls, blast (i.e., conference) calls, the NERC RCIS system, NERC Hot-Line, satellite phones, and other forms of telecommunication capabilities.

Business Continuity

In order to ensure business continuity for all potential system conditions, control center operators have an Operating Plan ("Plan") in place to address the loss of control center capability. This Plan will include requirements for items such as annual testing (in accordance with NERC standard EOP-008-1), periodic testing of infrastructure failover schemes (as needed), and applicable training. In addition, model changes, maintenance activities, and troubleshooting activities provide informal testing of failover schemes that will be used during control center evacuations. Many existing processes and procedures call for the failover of infrastructure to backup sites in order to alleviate issues on the primary system, providing opportunities for the testing of control center evacuation and transition of key infrastructure and operating capabilities. Many different subsets of evacuation processes can also be tested and validated during abnormal operating conditions.

Conclusion

The continued availability of control center infrastructure and operating capabilities is the primary element in maintaining reliable operation of the BES. Although a variety of methods exists across the industry, control centers and key infrastructure capabilities are commonly designed and implemented to provide multiple layers of defense. This includes primary systems, backup capabilities, and operating plans that facilitate coordinated interconnected operations. Due to the significance and complexity of these systems and their configurations, operating entities have documented plans to address loss of critical capabilities and to facilitate coordinated operations, even during extreme conditions. These plans are developed in accordance to NERC standards, often exceed minimum requirements, and are incorporated into System Operator training plans to promote the reliable operation of the BES.

It is imperative that these operating capabilities remain available under all operating scenarios. It is impossible to suggest all potential scenarios have been addressed with the variety of system designs and operating plans in place. However, the primary and backup capabilities in place today across the industry have integrated multiple layers of defense to help promote the continued reliable operation of the BES during most expected operating scenarios for an entity. This is coupled with the defense in depth that RCs provide by monitoring the same areas as TOPs and BAs to provide a high degree of resiliency to grid reliability.

North American Transmission FORUM

Open Distribution

Bulk Electric Systems Operations absent Energy Management System and Supervisory Control and Data Acquisition Capabilities—a Spare Tire Approach

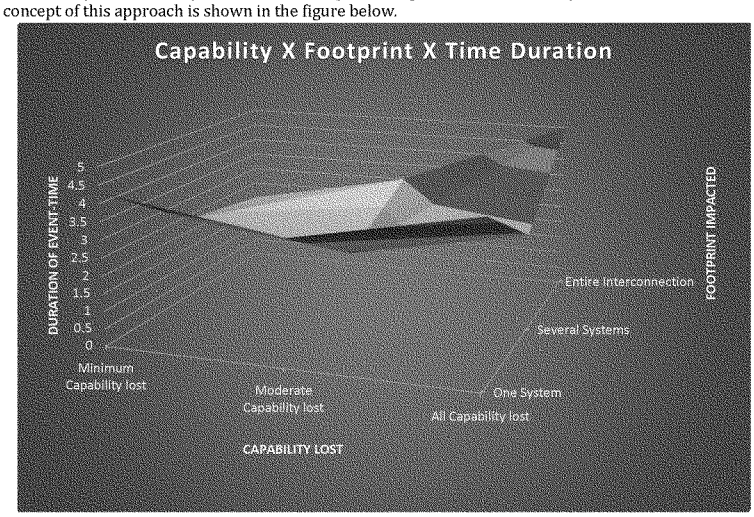
Disclaimer
This document was created by the North American Transmission Forum (NATF) to facilitate understanding of bulk electric system monitoring and control backup capabilities. The NATF reserves the right to make changes to the information contained herein without notice. No liability is assumed for any damages arising directly or indirectly by their use or application. The information provided in this document is provided on an "as is" basis. "North American Transmission Forum" and its associated logo are trademarks of the NATF. Other product and brand names may be trademarks of their respective owners. This legend should not be removed from the document.

Open Distribution
Copyright © 2017 North American Transmission Forum. Not for sale or commercial use. All rights reserved.

This NATF Reference document, representing research performed by industry personnel who have in excess of 200 years of cumulative experience, is in response to a question originally raised by the Electric Subsector Coordinating Council (ESCC) regarding how electric utilities would continue to operate during an event causing loss of both primary and backup control systems (i.e., total loss of the Energy Management System (EMS)/Supervisory Control and Data Acquisition (SCADA)). This concept was subsequently characterized as a "Spare Tire" approach to ensure continued system operations following the loss of critical applications. As such, this document[3]:

- Captures the results of an assessment of what operating strategies and reliability tools are present today for Bulk Electric System (BES) operations during times when traditional tools for situational awareness, system control, balancing and communications are unavailable, both internally and coupled with external loss of capabilities
- Identifies future areas of industry work and research to better enable operations during scenarios where there is a total loss of all EMS/SCADA capability

The scope of the event assessed was a complete loss of EMS/SCADA where the extent of condition expanded across multiple regions for multiple days. This approach (Capability x Footprint x Timeframe) was necessary to evaluate the impacts on operations and industry readiness. The concept of this approach is shown in the figure below.



[3] A companion NATF Reference Document- *Bulk Electric System Monitoring and Control - An Overview of Backup Capabilities*, provides an overview of the key capabilities for the reliable operation of the BES, along with a description of the various approaches used within the industry to ensure redundancy for critical capabilities so that System Operators are able to continuously monitor and control the BES in the event of the loss of the primary control center capabilities.

In performing the assessment, the team identified 11 key capabilities needed for system operations in the event of loss of EMS/SCADA. These capabilities were included in a limited industry survey in order to (1) determine their rank in priority for "Spare Tire" operations and (2) understand the levels of redundancy generally associated with each. The results indicated the following:

Priority Rank Order
1. External Voice Communications
2. Internal Voice Communications
3. Area Control Error Calculation
4. Frequency Telemetry
5. Transmission System Monitoring and Control
6. Generation Dispatch and Automatic Generation Control
7. Personnel Deployment (Human Remote Terminal Unit)
8. State Estimation / Real-Time Contingency Analysis
9. Interchange Scheduling
10. Off-line Power Flow Analysis
11. Load and Wind Forecasting

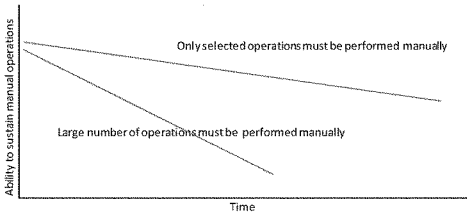
The ability to communicate was the highest ranked capability from the survey. This suggests the importance of having a robust communication network along with sufficient operating protocols available to enable effective communication with internal personnel, neighboring utilities, emergency responders, and other impacted stakeholders. The NATF survey also indicated that at least half of the respondents have implemented redundant capabilities beyond primary and secondary redundancy for the four highest ranked capabilities. At the same time, the results highlight other primary capabilities that remain critical for "Spare Tire" operations that may not generally employ redundancy beyond secondary levels.

Another key observation of the team is that any replacement of EMS/SCADA systems with alternate methods, such as involving humans, trucks, telephones, etc. would be:

- Limited in capability – the system will not function with comparable levels of efficiency and reliability
- Limited in time frame – given the personnel constraints and comparative inefficiency of this form of operation, it cannot be maintained indefinitely
- Resource-consuming – the same personnel who would be working to restore the system (along with ongoing forced outages) will be called upon for this type of operating environment
- Procedurally limited – it is possible that response and recovery procedures generally do not thoroughly define detailed responses to long-term events as described in the document.

It is of the utmost importance that utilities consider not only the availability for resource deployment but also the plans and protocol necessary across the entire enterprise to effectively execute this capability for prolonged periods. This includes the identification of critical skills

needed to operate the grid in this manner in addition to the training requirements for any personnel needed to perform tasks consistent with manual operation. This degradation of the ability to sustain manual operations is shown in the figure below.



Due to the various event scenarios possible, it was concluded that a single recovery method is not appropriate to address all events rendering an EMS/SCADA unavailable. However, as part of the review process for considering a "Spare Tire" strategy, consideration was given to principles that help prepare for and respond to multiple types of high-impact, low-frequency events. The following operating principles were found to be common across multiple entities based on shared experiences, similarities between procedures, and ranked responses for key capabilities.

- Understand impact and plan for personnel safety, training, and coordination
- Ensure availability of alternative communication capabilities
- Consider greater levels of redundancy for primary operating capabilities
- Ability to notify stakeholders and request (or lend) assistance
- Comprehensive and clear logistical plans for personnel and data distribution
- Understand and plan for resource implications (field, engineering, operations, etc.)
- Codify and practice concepts for "Spare Tire" operations
- Consider strategies that mitigate multiple high-impact, low-frequency threats

As for next steps to even better position the industry to address a "Spare Tire" scenario, the team identified the following areas for future work:

- Continue to address voice and data communications- Lead: DOE/National Labs/EPRI
- Develop additional Reliability Tools/Data Availability to aid situational awareness during a "Spare Tire" event- Lead: DOE/National Labs/EPRI
- Formalize strategies and plans for "Spare Tire" operations scenarios- Lead: Individual utility companies
- Formalize data sharing on "Spare Tire" operations strategies- Lead: NATF
- Harden EMS hardware components and develop streamlined EMS recovery process and capabilities- Lead: EMS vendors

It should be noted that individual company practices may vary from descriptions provided in this document. Also, this document does not create binding norms, establish mandatory reliability standards, or create parameters by which compliance with NERC Reliability Standards is monitored or enforced.

Bulk Electric Systems Operations absent Energy Management System and Supervisory Control and Data Acquisition Capabilities—a Spare Tire Approach (2017)

The CHAIRMAN. Thank you, Mr. Galloway.
Mr. Yardley, welcome.

STATEMENT OF TIMOTHY M. YARDLEY, SENIOR ASSOCIATE DIRECTOR OF TECHNOLOGY AND WORKFORCE DEVELOPMENT, INFORMATION TRUST INSTITUTE, UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Mr. YARDLEY. Good morning, Chairwoman Murkowski, Ranking Member Cantwell and distinguished members of the Committee. Thank you for the opportunity to speak today.

My name is Tim Yardley, and I'm a Senior Researcher and Associate Director at the Information Trust Institute at the University of Illinois, Urbana-Champaign. My research focuses on cyber resiliency and critical infrastructure.

Let me start by saying the cyber threat to the grid is real and the threat of potential blackstart is here. The time to act is now.

It is critical that the Committee understands the following. Much existing work has already been done and that work is tremendously important; however, we need to think broader about what it means to be cyber resilient. We need to focus on increasing the skills and capabilities of our people as much, if not more, than we focus on the technology, and we need directed funding and test beds to realize that. We need to think through the policies, procedures, people, skills, tools and the requirements necessary for those items to function before they are called to action. And lastly, these capabilities can be achieved only if academia, industry and government work closely together in focused research, development and education programs and funding should increase to support past successes, like those at the University of Illinois, and to create new ones elsewhere.

With that in mind, even if there remains work to be done, I rest assured that our nation is relatively prepared to address the logistics of a traditional blackstart scenario. The dedicated commitment of all of the first responders, echoed in the rest of the panel today, to pull together is second to none. I fear, though, that we are still not prepared to do so in the face of a cyberattack that eliminates our ability to trust the systems that we use to operate and restore our grid. There is urgency necessary in closing that gap. The risk is growing and all of us involved know it. But we must put our best minds on solving it.

As you have heard in prior testimony, cyber resiliency aims to protect through established cybersecurity techniques but acknowledges that such protections will eventually fail. For over a decade now, much attention and funding has been placed on cybersecurity for the grid, but cyber resiliency is much more than just cybersecurity and it's only recently gaining real focus. The prior investment in cybersecurity has been well spent and there is continued need, but we must go further. We must understand what happens when those protections fail us.

One of my most relevant research efforts falls under the DARPA RADICS program, which stands for Rapid Attack Detection, Isolation and Characterization Systems. The goal of that program is to enable blackstart recovery of the power grid amidst a cyberattack.

RADICS research is developing technology that cybersecurity personnel, power engineers and first responders, such as the National Guard, can utilize to accelerate restoration of cyber-impacted electrical systems. This is not a tabletop. This is real technology being tested in the field.

One of the key tenants in this program, and part of my role, is the development of test bed environments that enable exactly that and aiding in the creation of the exercise format that enables the evaluation and improvement of those technologies as they are developed before they are called to action.

By creating these environments and developing scenarios that allow practitioners to put these tools to work, great progress can be made on preparedness as we continue to invest in cyber resiliency. This effort, along with years of prior work funded by DOE OE CEDS, provides me with direct experience in understanding where the tools that we have built succeed, and where they fail us.

I look at test beds and many look at test bed environments as a piece of a bigger puzzle but as an area of focus on their own. That needs to change. And the full potential of test beds and their capabilities need to be realized to advance our state of security.

Imagine a facility that allows for testing our systems in unprecedented ways, that enables innovative training for our current and future workforce, that exposes our system to sophisticated attacks and allows us to understand what they look like and how to address them in practice, that puts our policies and procedures to task and does all of this repeatedly in days or weeks, rather than months, years or decades.

This system also needs to be flexible. It needs to adapt to the needs, the system's understudy and the adversarial threat landscape as it evolves.

We must be prepared and test beds can help us do that, but such a facility does not fully exist today. Great strides have been made in academia and national labs, and with the right combination of funding and people it can be fully realized.

We are only as strong as our weakest link and when put into the context of cyber resiliency for the grid, that weakest link is likely our staffing. Many organizations have cybersecurity-focused staff on hand, as well as third party entities contracted to full response actions. In the end, however, we simply do not have enough people to deal with a large-scale attack. Even if we put our best people on the ground, without the right tools and practiced skills of using those tools, they will be inefficient at best in the face of a determined and sophisticated adversary.

We can and should put money into technology, but without the people to leverage it appropriately, we are still at a loss. We must invest more in our people. We have to think outside the box and we have to innovate in how we train people. Staffing in a large-scale emergency response is often one of the most difficult undertakings, so we need to address it proactively and increase the breadth of resources now. Only together can we solve these problems.

Thank you.

[The prepared statement of Mr. Yardley follows:]

Timothy M. Yardley, Senior Associate Director, Information Trust Institute, University of Illinois Urbana-Champaign

Testimony of

Timothy M. Yardley

Senior Associate Director of Technology and Workforce Development, Information Trust Institute, University of Illinois at Urbana-Champaign

Before the United States Senate Committee on Energy and Natural Resources

October 11, 2018

Introduction

Good morning Chairwoman Murkowski, Ranking Member Cantwell, and distinguished Members of the Committee. Thank you for the opportunity to speak today.

I am a Senior Researcher and Associate Director at the Information Trust Institute, University of Illinois Urbana-Champaign. My research focuses on cyber resiliency in critical infrastructure with a particular focus on the electric power grid. I also have a deep prior background in telecommunications and cyber security in a broad number of disciplines. I have worked on cyber resiliency research for critical infrastructure for over 10 years with funding from DOE, DHS, DARPA, and Industry. Much of the electricity subsector knows me based on the extensive testbed capabilities that I have built up at the University of Illinois and that have been a building block of many scientific advances made in this domain.

I have proposed and participated in a variety of research projects that have materialized into technology that is deployed on our electric grid today. I have been funded to work on areas covering the gamut of identification, protection, detection, response, and recovery. I have also been active both in assisting in the education of new minds through student interactions and in adapting existing workforce to the evolving modernization of a cyber resilient grid. Lastly, some of my current work focuses on providing portable testbed environments that allow for the verification, validation, and improvement of mission-critical cyber response tools aimed to aid in black-starting the electric grid amidst a cyber-attack. In short, my experiences provide me with a unique perspective to offer the Committee insight and recommendations concerning the cyber recovery of our grid when faced with a full or partial black start scenario.

In my remarks today, I will:

- Describe a broad viewpoint on cyber-preparedness for restoring the electric grid,
- Describe a need for research, development, and continuous engagement of both preventative and restoration toolsets,
- Describe the unique contribution universities (including the University of Illinois) play in developing new, innovative technologies and approaches to preventing, detecting, and recovering from cybersecurity threats to the grid,

Timothy M. Yardley, Senior Associate Director, Information Trust Institute, University of Illinois Urbana-Champaign

- Emphasize the need to increase investment and innovate in approach for workforce development cyber-preparedness,

- Emphasize the need for more robust rehearsal of policy, skills, tools, and knowledge acquisition to carry out our global goals

Background

It is not news to anyone in this room that the critical infrastructure that is relied on throughout the world is under threat. In the news are many reports of information gathering and potential attacks against this infrastructure, including the electric grid. Cyber security researchers are uncovering campaigns, toolsets, and even some attacks that are targeting electric grids and the systems that operate them. It is also well understood that a compromise of the power grid control system or other portions of the grid's cyber infrastructure can have serious consequences, ranging from a simple disruption of service with no physical damage to potential permanent damage that can have long-lasting effects on the ability of the system to operate.

I rest assured that our nation is relatively prepared from a physical perspective to address the logistics of a traditional outage or black start scenario. I fear though, that we are still not prepared to do so in the face of a cyber-attack that eliminates our ability to trust the systems we use to operate our grid. There is urgency necessary in closing that gap.

Cyber Security Funding

For over a decade now, much attention and funding has been placed on cyber security for the grid, but cyber resiliency is much more than just cyber security and is only recently gaining focus. That money has been well spent and there is a continued need to fund the protection of our electric grid from adversarial manipulation. However, as has been shown repeatedly in the media, a determined adversary will eventually succeed, so what do we do then? While the attacks of the past were often focused on the business side, it is becoming more concerning that the toolsets are migrating to operational technology (OT) specific functionality. Are we prepared? Unlike the examples so far in the media, the U.S. grid is arguably more resilient to failure but just because it is harder to topple, doesn't mean that it isn't possible. Cyber Resiliency as an approach, is a potential answer.

Given that protection cannot be made perfect, and the risk is growing, cyber resiliency is critically important. Cyber resiliency aims to protect through established cybersecurity techniques, but acknowledges that such protections can never be perfect, and requires monitoring, detection, and response to provide continuous delivery of electrical service. While some solutions from classical cybersecurity can support cyber resiliency (e.g., intrusion detection and response), the majority of the cybersecurity work to date has focused on preventing the occurrence of successful attacks, rather than detecting and responding to partially (or fully) successful attacks that occur.

One of my most relevant research efforts falls under the DARPA Rapid Attack Detection, Isolation, and Characterization Systems (RADICS)[1] program lead by Mr. Walter Weiss. The goal of that program is to enable black start recovery of the power grid amidst a cyber-attack on the U.S. energy sector's critical

[1] https://www.darpa.mil/program/rapid-attack-detection-isolation-and-characterization-systems

infrastructure. RADICS research is developing technology that cybersecurity personnel, power engineers, and first responders can utilize to accelerate restoration of cyber-impacted electrical systems. One of the key tenets in this program, and part of my role, is the development of testbed environments and aiding in the creation of an exercise format that enables the evaluation and improvement of these technologies as they are developed. By creating these environments and developing scenarios that allow practitioners to put these tools to work, great progress can be made on preparedness as we invest in cyber resiliency.

In current viewpoints, many look at testbed environments as a piece of a bigger puzzle, but not as an area of focus on its own. That needs to change and the full potential of testbeds and their capabilities need to be realized. Imagine a facility that allows you to test your theories and new techniques on systems that truly operate like the real world, but without the capital and time expenditures necessary to deploy those on the real system. Imagine a facility that allows next-generation products to be configured, tested, and validated iteratively during development to build a more robust product and a stronger overall solution. Imagine that same facility being used to train your current and future workforce on the systems they use in the real world, with behaviors that match, with their own configurations, and do so in matters of days or weeks rather than months or years. Imagine that same facility being used to continuously train our first responders so that they are prepared when they are called upon. Now, use that facility to look at these scenarios in face of adversarial manipulation and TTPs. Such a facility doesn't fully exist today, but great strides have been made to realize aspects of that at the University of Illinois as well as at DOE National Laboratories. Much more work still needs to be done and with the right combination of teams, it can be realized.

Testimony has been previously given to this committee on the importance of cyber resiliency, so I will not repeat that here. I do echo the importance and necessity of that path. Testbeds are a cornerstone of understanding how we are improving on cyber resiliency as we progress down that path. Instead of focusing on resiliency though, I will focus on some specific aspects that may help as we continue to harden our systems that protect critical infrastructure.

Focus on Exercising Essential Items

With FAST Act authority, there are new powers for taking action when action needs to be taken. There remains a question as to what those actions may be and when they are appropriate to take. Recent work by Paul Stockton[2] and others have identified needs to look at templates and think through the scenarios that make sense for leveraging these powers and putting the right protections in place. This is a critical piece that will take time and effort to work through, with a variety of stakeholders at the table. This is time that must be spent.

Cyber security workforce education is another area that takes time to work through. There is a saying that we are only as strong as our weakest link, and when put into context of cyber security that weakest link is likely our staffing. Many organizations will have cyber security focused staff on hand as well as third-party entities that are contracted for response actions. Are there enough of them? Are they truly prepared to respond to a critical infrastructure attack at scale? What about the national guard and others that can be called upon? How do we make sure all of these people have the tools, skills, knowledge, and pre-existing relationships so that if an emergency black start cyber-involved scenario

[2] http://www.jhuapl.edu/Content/documents/ResilienceforGridSecurityEmergencies.pdf

ever occurs, they are ready to hit the ground running? How do we guarantee that their skills are fresh and not "rusty" from lack of use? This is a difficult problem that traditional training can't fully prepare one for, so we have to think outside the box and we have to evolve how we train people. Testbeds are a partial solution, but more focus is needed to advance that further and it still needs a pipeline of people. Staffing in a large-scale emergency response is often one of the most difficult undertakings, so we need to address it pro-actively and increase the breadth of resources now.

What do you train the people on though? The base systems will need training, of course. The traditional cyber security and forensic response tools as well. What about those tools that are built for cyber-physical environments like the electric power grid? Further focus needs to be spent on assembling what that toolkit looks like and to fill the gaps on what is missing. Some work is being done in this space, but more focus needs to be placed on it.

Academic Involvement (NSF/DOE/DHS/DARPA)

Many of these cyber-resilience findings being discussed today have grown out of collaborative academic-industry-government settings, including several major research activities that I have led or participated heavily in. Funding for these efforts has been broad, indicating both the importance and the complexity of these problems. In my time in this area, I have been involved in funding from Industry, NSF, DOE, DHS, and DARPA all taking on a particular piece of this problem space. Some of those efforts include the Trustworthy Cyber Infrastructure for the Power Grid projects (TCIP, 2005–2010; and TCIPG, 2009–2015), the Critical Infrastructure Resilience Institute (CIRI, 2016-2020), the Cyber Resilient Energy Delivery Consortium (CREDC, 2016-2020), and the Cyber Physical Experimentation Environment for RADICS (CEER, 2016-2020).

It is my belief that we must not just innovate but that we must put into practice the knowledge that comes and the tools that are created. Once knowledge is disseminated and tools are created, they must continue to use these tools regularly so that the tools can continue to improve and advance rather than be behind the glass and not touched until they are needed. All of these are partnerships between academic institutions, national labs, government sponsors and stakeholders, and most importantly with Industry. Across these efforts, the team of collaborators have worked together to understand, improve, and enable critical work across the target critical infrastructure domains. In both technology and impact, each of these have had their own successes including creating multiple startup companies and transitioning multiple technologies to industry (including Grid Protection Alliance, First Energy, Schweitzer Engineering Laboratories, ABB, Honeywell, Ameren, Telecordia, GE, Entergy, EPRI, DTE Energy, and PJM, among others). The projects also have had a significant positive impact on workforce education, delivering successful short courses, producing graduates, conducting hands-on training, and providing the base knowledge necessary to do this type of work by others.

While progress is being made, further work is critically needed to define cyber resiliency architectures that protect against, detect, respond to, and recover from cyber-attacks that occur. Some specific guidance about cyber resiliency research that is critically needed comes from a consensus study published in July 2017 by the National Academies of Sciences, Engineering, and Medicine entitled "Enhancing the Resilience of the Nation's Electricity System."

Timothy M. Yardley, Senior Associate Director, Information Trust Institute, University of Illinois Urbana-Champaign

Summary

The cyber threat to grid resiliency and the reality of a potential black start scenario is real, and the time to act is now. It is critical that the committee understands the following:

1) A lot of existing work has been done, and that work is tremendously important. However, our effort needs to think broader and look at the problem from a cyber resiliency perspective rather than just cyber security.

2) We need to focus on increasing the capabilities of our people as much, if not more, than we focus on our technology.

3) We need to think through the policies, procedures, people, skills, tools, and the requirements necessary for those items to function before they are needed.

4) These capabilities can be achieved only if academia, industry, and government work closely together in a focused research, development, and education program.

5) Congress should continue to fund and increase funding to DOE and other government agencies to advance this research with broad engagement between Academia and Industry, building upon successes of the past.

Thank you for the opportunity to be here with you today. I would be happy to answer any questions that you have.

The CHAIRMAN. Thank you, Mr. Yardley.

A very important reminder at the end that with all the technologies, it is still the human beings that we need to have on the ground working through so many of these. I appreciate that.

This has been a great discussion, really. I thank you all. You clearly have identified where these vulnerabilities are when, if we were to have a significant crisis and this whole issue of blackstart, where is the vulnerability? Are you able to test as you need? Are you able to communicate during the time of the disaster? The vulnerability of being reliant on a single fuel source. The cost, the people, the trained individuals. So again, very good conversation.

I want to start my questions off about the reliance on a single fuel source for blackstart. The joint NERC and FERC report that many of you have cited cautions us against reliance on a single fuel for blackstart capabilities. But do we have a sense as to how many blackstart power plants actually rely on a single fuel source? And if we can identify that, what progress are we making then toward diversification for multiple fuel sources? Dr. Ortiz, since you raised it, and Mr. Ott, you have been very involved with it, if you could speak to that.

Also, I am curious to know more how hydropower can play into this fuel source as that alternative. As Senator Cantwell has mentioned, she is blessed with extraordinary hydro resources, but when you think about a fuel source, a ready fuel source that is just sitting there with a level of availability that, perhaps, you don't see with outside fuel sources like storage of diesel or gas. So if you could speak to that, both of you.

Go ahead, Dr. Ortiz.

Dr. ORTIZ. Yeah, thank you very much, Madam Chairman.

By way of introduction, let me note that in our study, one of the key recommendations was that an entity identify areas where its blackstart generators depend on a single fuel source——

The CHAIRMAN. Okay.

Dr. ORTIZ. ——and look toward options for mitigating the potential risk of that fuel source not being available. There are a number of ways in which to do this. They could include firm contracts with alternative fuel sources, as well as working with local regulators to ensure appropriate air permits for, say, diesel or other fuels to be used.

Unfortunately, with respect to specific resources and specific plans, given that our study drew upon the anonymous participation of a number of utilities, I can't speak to any specific cases. However, in general, the study team, in looking at some of the best practices at the participating utilities, saw that those that had sought, that those that had identified this risk, had been able to identify means in which to mitigate it.

The CHAIRMAN. Mr. Ott.

Mr. OTT. Thank you, Senator Murkowski.

The issue—we have raised the issue and, certainly, talking about the issue of single fuel dependence, it's not only on blackstart but more globally, I think. So what we've addressed is we've started a process to have a discussion with our stakeholders. I don't think it's a widespread issue, meaning 50 percent, but there is some vulnerability there.

So we are addressing it through our request for proposals that we issue for blackstart services. We are addressing it through discussions with stakeholders. The reality check is it becomes more expensive when you ask for more fuel diversity. But certainly units like hydro and other diverse units, whether it be the combination of solar and battery that's still experimental, but it's those types of things that will help reduce the cost and similarly with other types of fuel security questions. As long as you identify the service and don't fall into the trap of saying I want a specific technology and I want to save a specific type of plant, then it becomes a little less expensive. But certainly, we're on it. I would say, certainly it is a vulnerability, but it's not a widespread vulnerability.

The CHAIRMAN. But it is a vulnerability that you are highlighting and not directing these are your preferred alternatives. It is what works for you within the region for that particular utility.

Mr. OTT. And what's key is we're stating the requirement is fuel security and a diverse, you know, no dependency, no single point of failure. So the requirement is not you have to be oil, or you have to be gas, or you have to be hydro, and I think that helps lower the expense because you're allowing more diverse resources to come in and provide the service and the service is security of supply, essentially.

And for blackstart, you know, we don't want to have a single point—I mean, if the system is going down and you have very few options, you don't want that single point of failure to rear its head in a surprise and, certainly, we are on that and we are taking action.

The CHAIRMAN. I appreciate that.

Senator Cantwell.

Senator CANTWELL. Thank you, Madam Chair, and I thank the witnesses. You have all provided—I think I could ask a thousand questions—but I will try to be focused.

You brought up some really good points, and I would say just from my own experiences in the State of Washington, we had a horrific slide that killed 40 people, called "the Oso," that basically cut our community and response in half. Literally, we did not have broadband communication nor the ability to get to the community because the slide isolated everybody. You literally had to drive around three hours to just communicate with the individuals. It made the response and the recovery so challenging, and we have had other natural disasters in our state that just bring up this entire communication element of the response.

Ms. Ditto, you mentioned that, and Mr. Yardley, you mentioned it. Mr. Galloway, you mentioned it too. What do we need to do on the communication side to make sure that the work on the restart is coordinated as well? Because I think this is something—I know that movie Blackhat. I mean, they literally were—or wait a minute, not Blackhat. I think it was the Bruce Willis movie, Live, whatever it was called, something Live Free, Die Hard.

[Laughter.]

But he—I have watched many of these cyber—but anyway that was——

Senator GARDNER. Stapleton Airport, just for——

Senator CANTWELL. ——that was a fire sale issue.

But the point was that they had to go to the ham radio operators, like the only people left to communicate were the ham radio operators.

What do we need to do on the communication side here?

Ms. DITTO. Thank you, Senator, for that question. I can lead off, if that's okay?

So, first of all, I'll just say, just, sort of, state the obvious. Digital communications is why we have a cyber vulnerability in the first place. But those same digital communications enable a much greater efficiency in our grid that enables variable energy resources and other types of resources that we all care about and want, including battery storage and solar rooftop and some of the things on the edge of the grid.

So there are some really positives about communication, but they also create vulnerabilities that we have to manage that risk over time, including doing some of the research that was suggested by Mr. Yardley.

But when it comes to this idea of a real Black Sky event or a blackstart restoration event, as I mentioned in my testimony, utilities themselves own and operate their own networks, in most cases, because the traditional communication carriers just aren't willing or able to provide the level of reliability that's needed by utilities in these situations.

So if digital communications are lost because of a cyberattack or because of some other situation where your fiber lines are cut or something like that, we still can default in most cases to voice communications over radios, kind of like you were mentioning with the ham radio situation. We have microwave-based systems that we've built and maintain and we have backup power for them because communication systems require electricity to operate. So we have backup power generation and fuel onsite. Some utilities have fuel onsite for those backup power generation—backup power generators for their communication systems of 6–10 days. And that's part of a standard that the utility has developed, the fuel onsite for those backup generators, for communications only.

There are things we're doing already, but some of these policy areas could be addressed.

Senator CANTWELL. Well, I wish, and I want to hear from Mr. Yardley, but I wish we would address these because we have real life examples now. We can go back to our Carlton Complex fire where the Okanagan Valley was basically on fire. The communication lines burned up, and you could not even communicate with individuals.

I think we have some test beds, but I want to hear from Mr. Yardley about your thoughts.

Mr. YARDLEY. I think there's really two key issues.

One is the physical attack on the communications, blocking spectrum, radios not being available, lines being down, et cetera, due to issues from that perspective. But there's also the cyber. What if they're all there, but you can't use them because you can't trust them? They've been attacked themselves. So what do you do then? And further, how do you—it's one thing to support the normal operations, but how do you support the forensic response as well? How do you enable that channel of communication which may be

completely different than traditional operations and at the same time, your number one priority is to support the normal operations, but you have to weigh that against the ability of forensically communicating to be able to support that operation and enable it in the first place?

The second aspect is that with comms under attack themselves, we're good at defending our communications networks, right? The internet is defended everyday from attack and subversion, but we see it happen still. So what's to say that an adversary would not do that when they were attacking the grid, that they wouldn't have a multipronged attack that attacks not just the grid, but also attacks the communications as well?

So we have to think about it broader, not just in the aspect of are comms available, but can we trust those comms? Is the adversary listening? Is the adversary manipulating those communications while we go?

Senator CANTWELL. Do we have enough resources here? How do we get a full understanding of the resources needed? I mean, you are coming to us, you know, the home of mosaic and producing, really, what translated the DARPA information into a browser. What else do we need to do to give institutions like you and others the resources?

Mr. YARDLEY. Well, I think that's a difficult thing, right? There are people that are needed, right? The people that can train the material that they need to train about and adapting that. But there's also gaining the interest. The aging workforce has been reluctant, in some ways, to engage in some of the more modern technologies and you're seeing that adaptation come in with the younger workforce coming to market. But they don't have the background that the existing workforce does on the rest of the systems.

And how do you marry those two together, where you have people that are trained on the physical aspects of the system but that are also as well versed on the cyber aspects of the system? How do you create that hybrid? We've been trying to do that for years at the University of Illinois in collaboration with a lot of other academics, but it's a very difficult problem to solve.

And I think test beds are a way that you can help do that, by getting people hands-on experience with these types of stuff so that they can actually say, alright, look, I am doing my physical function that I have, but I have these cyber operations that I have to deal with and understand and address at the same time.

Senator CANTWELL. Well, I know I am way over time but, Madam Chair, I think we should have a WPPA program for cybersecurity. We should just say, calling all Americans, we will help you get educated in this area if you help us. I think there are a lot of young people in the Northwest, if they heard that call, who would respond to it. I mean, we get cheap hydro, we get cyber, we get the internet. But we need to sharpen our call that we need them and we need them to respond to this. We need thousands, hundreds of thousands of people in this infrastructure call. So I hope we can figure out a way to promote that.

The CHAIRMAN. Thank you, Senator.

Senator Gardner.

Senator GARDNER. Thank you, Madam Chair. Thank you to all the witnesses for your testimony today and your great work in this field.

I am particularly pleased to have Mr. Torres joining us today from the National Renewable Energy Laboratory and also particularly pleased to have him here because of his hometown, La Junta, Colorado, a small town in Eastern Colorado. To see a small-town Colorado kid of the Eastern Plains grow up and run a laboratory with world-renowned scientists is pretty doggone exciting and says something great about this country. So thank you very much for your leadership and for being here.

I will start with you and the questions that I have.

We had a chance to visit both at NREL when Secretary Perry made the visit a couple of months ago to Golden and, obviously, in the office this morning, we had a chance to talk. We talked about resiliency. We talked about our electric grid. Your understanding of the grid and the potential we face for significant blackouts and, you know, we had some power outages just this past weekend. It started snowing in Colorado, so the ski slopes will be open. We are preparing for that. Get your tickets now. Everybody can reserve those hotel rooms. But we are starting to see—we had some blackouts, right, because we had tree branches falling on the power lines and some of that first snow. We are talking about events that could be catastrophic, not just a neighborhood that is out, and what that could mean long-term.

What areas of research do you see as most vital to our nation to avoid risks of these blackouts, catastrophic-style blackouts? What area is most vital for our nation to avoid these risks? How do we quickly and effectively recover from these types of occurrences?

Mr. TORRES. I think there's opportunities in some technologies, in distributed generation. Energy storage, I think, is a big area, especially coupled with some of the new renewable sources that actually are becoming more abundant, like solar and wind, specifically.

I think there's a need for more research around inverter controls and how you actually network some of these various devices in a consistent way, replicable way.

I think there is opportunity to see how we can better get inverter-based technologies to interact with the traditional inertia-based generators as well.

And, of course, the cybersecurity aspect, I think, is still really important. We need to understand that much better. As we bring in some of these technologies that have not traditionally been used for blackstart, we may need to—we need to start looking at supply chain challenges there because they have not been on the list for that. So——

Senator GARDNER. Supply chain challenges in terms of cybersecurity? Where those products are——

Mr. TORRES. Exactly.

Senator GARDNER. ——and other things?

Mr. TORRES. Absolutely.

I think there—because the focus has been on a lot of the technologies that have traditionally been part of blackstart. As we start to incorporate some of these new technologies, that has to be on the list as well and understanding the life cycle supply chain.

Senator GARDNER. Thank you.

Senator Murkowski, I think, talked a little bit about hydropower and the application for hydropower in this scenario.

If hydropower is going to be an effective tool in such an incident, are we talking about the applicability of micro hydro, small hydropower projects? Are we talking about significant-sized, pump-backed projects like we have at Twin Lakes in Colorado?

Mr. TORRES. Right. So I think hydropower can play an important role in blackstart. It's one of the most economically effective and efficient generation sources for blackstart because it does not need a lot of power to get its turbines running as you might need for some of these other generation types. I think where it is an abundant resource, where water is an abundant resource, it makes tremendous sense. We don't have that everywhere, but I think there's opportunity at different sizes.

Senator GARDNER. At different sizes, so a smaller project works just as well as a bigger project?

Mr. TORRES. They could potentially support at smaller sizes as well, absolutely.

Senator GARDNER. Very good. Thank you. Thank you for that.

Dr. Ortiz, I was interested in the studies that you mentioned and your study that you talked about, the joint study. A team recommended utilities prepare for widespread blackouts by talking about the vulnerability of backup power, adequacy of communications, personnel requirements, perform manual restoration activities without EMS or SCADA. Have the utilities completed those assessments? Are there any early results that you can share?

Dr. ORTIZ. Thank you for the question, Senator.

I should note that the study made these recommendations to the utility industry based upon our review of their restoration plans, looking specifically at their ability to restore their systems without access to SCADA, EMS or other communication means or traditional communication means.

I thank the eight utilities that participated with us. However, this was not a compliance exercise, nor a specific compliance, set of compliance guidance, but rather just a set of recommendations. So, in particular, the staff has not followed up with the general industry on these topics. If you'd like I can go back to the team leaders, as well as our partners at NERC and the regional entities to see if they have learned anything in addition.

Senator GARDNER. Thank you very much, Dr. Ortiz.

Ms. Ditto, the comment you made, I believe, talking about FCC and FERC, and I'm out of time, so quickly. There is some communication or is there none?

Ms. DITTO. You know, that's actually a better question to FERC, but I don't think there is any kind of formal communication between the two agencies right now.

So we would ask that to be formalized in some way, whether through an MOU or a less formal process like they undertake with the NRC. There are some precedents for that because they really do need to understand each other, and we're not sure that that situational awareness is occurring from either agency right now.

Senator GARDNER. Great. Thank you.

The CHAIRMAN. Thank you, Senator Gardner.

Senator Manchin.

Senator MANCHIN. Thank you, Madam Chair, and thank you all for being here.

My first question is going to be about blackstart itself. How many megawatts of blackstart capacity do we have in the United States? If anyone can answer that? And then, how many megawatts of blackstart capacity do we have in PJM?

Mr. Ott.

Mr. OTT. Thank you, Senator Manchin.

Again, blackstart is a very unique service.

Senator MANCHIN. Sure.

Mr. OTT. And so, as far as the total megawatts, it's much, much smaller.

Senator MANCHIN. Sure.

Mr. OTT. We're in the hundreds of megawatts type of——

Senator MANCHIN. Maybe I can ask the question a little bit differently.

Mr. OTT. Okay.

Senator MANCHIN. How many megawatts does it take to start up a plant? So let's use a 900-megawatt coal-fired plant. It goes down completely. The whole system collapses. How many megawatts?

Mr. OTT. Right. Generally speaking in a plant that size, you're probably looking at between 10 and 20 megawatts to get everything running.

Senator MANCHIN. To get it back up and running?

Mr. OTT. To get it moving.

But the point is, is there's other, you have to connect to it. You have to connect through the transmission to it.

Senator MANCHIN. Sure.

Mr. OTT. So there's some extra stuff there.

But you're in the hundreds of megawatts type for the system. But nuclear plants, of course, require a little bit more blackstart.

Senator MANCHIN. I am understanding that hydroelectric is the best backup system we have for blackstarts?

Mr. OTT. It certainly is a capable resource but my opinion is as, obviously, a very conservative power operator, I want diverse sets of resources. I want some hydro, some small gas, some small oil. I want some stuff spread around because you only have hydro in certain spots.

Senator MANCHIN. Anybody else on how much blackstart capability we have? Nobody? If anybody could find that out, I would appreciate it because I want to know how vulnerable we are.

We are talking about this and it has not happened, but we have had some historic blackouts and challenges over the years, and we could be in a very dire situation. I am concerned about the reliability of the grid.

Yes, sir, Mr. Ott.

Mr. OTT. I can just give you a little bit more information.

So we actually contract, PJM contracts on behalf of the region—remember we're about 25 percent of the U.S. So, we actually look at the plan, say how much do we need and we actually issue long-term or yearly or multi-year contracts to secure it.

I can tell you for PJM, we've secured what we think we need based on the blackstart plan. And again, not to say that we are done, there's more to do.

I think fuel diversity is an issue, meaning that we have an overdependence on one type. But I will tell you, we do, we've contracted——

Senator MANCHIN. Since I am in your system, PJM basically takes care of my State of West Virginia. We have put an awful lot of power into the PJM system.

A couple of things I wanted to address is, first of all, in 2009, the national average price of electricity was $0.0982 per kilowatt-hour. In West Virginia, it was $0.0784 per kilowatt-hour. Today, the national average is $0.1312 per kilowatt-hour. In West Virginia it is $0.1142 per kilowatt-hour, and we have more energy than we have ever had.

So something is causing the people who are struggling day-to-day, month-to-month, to pay a much higher price, and it doesn't make any sense to me whatsoever.

Also, at PJM you have a total of 4,266 megawatts that you are going to retire, 2018 through 2020. The average age of the retiring units is 43 years. The size is an average of 249 megawatts. Nine of those units, totaling 3,600 megawatts, are large enough that I would think at least some of these were probably relied upon during the bomb cyclone or all the other cyclones. What are you going to do when they go down? We have had this conversation before.

Mr. OTT. Yeah, so essentially for the units that are retiring, we've done a study and actually released that study to say that for our reliability criteria, the NERC reliability criteria, they can retire on schedule and not violate any of the criteria. However, one thing that I think is a very legitimate concern and question that's been asked by yourself and others is at what point, as we have coal and nuclear retiring and more and more dependence on gas, at what point would we, in fact, have what I would call a fuel security or an overdependency problem on a grid the size of PJM which would be a significant risk.

We will release a study on that very question, incorporating these retirements into that on November 1st. We will actually issue and say we've actually looked at this analytically, looked into the future, looked at even more retirements.

Senator MANCHIN. Let me just say, if I can——

Mr. OTT. So we are addressing the question.

Senator MANCHIN. My time is running, and anybody can answer this question here because we have been working on, and I am concerned about, the reliability. We have an awful lot of coal, natural gas, we have hydro, we have wind. We have been very blessed in West Virginia. We are, as you know, a big net exporter of power, and we do the heavy lifting. We don't complain about that.

But we worry about the resilience of our system. With that being said, I have been a big supporter of, basically, the Defense Act that makes sure that we keep the best of the best, as far as in coal-fired plants and nuclear plants that are up to specs and have the latest technology in operation, for at least two years until you can get through this because a lot of analytics are going on right now. If this all comes down and these retirements go into an accelerated

rate, I believe that the grid is going to be jeopardized, the security of our nation is going to be jeopardized.

What is you all's feeling as far as the Defense Act giving us the ability, at least a 24-month ability, to find out what direction we are going to go and how we get there? Anybody want to talk on that one?

Mr. OTT. I can certainly offer a comment.

I think the retirements in question have been announced. They're for 2021–2022 timeframe. Our analytics are looking at those timeframes and, certainly, I think we do have time, should we find a problem, to take action within our systems.

So by offering we would be, instead of the Federal Government stepping in, allow us to complete our analysis in the time given. But at this point—I'll yield back because it's time.

Senator MANCHIN. But my thing is, this basically makes no sense to West Virginians at all to produce as much power as we produce, to be paying higher prices that are unnecessary and having plants come offline that are basically gouging West Virginians. This is what they cannot understand. We have lower gas prices than we have had for the last 20 years. We are pumping more gas out of our state than ever before, and our people are paying higher prices. It makes no sense, sir. We are getting screwed.

Thank you.

The CHAIRMAN. Thank you, Senator.

Senator Hoeven.

Senator HOEVEN. Dr. Ortiz, how frequently do utilities have to test blackstart units to ensure they can function in the event of a system-wide blackout?

Dr. ORTIZ. I'm reading, actually, directly from the reliability standard. That's EOP–005, Version 2, Requirement 9 says, "Each transmission operator shall have blackstart resource testing requirements to verify that each blackstart resource is capable of meeting the requirements of its plan." These resources—"The frequency of testing such that each blackstart resource is tested at least once every three calendar years."

Senator HOEVEN. Is that enough?

Dr. ORTIZ. It is what the reliability standards—the way that they are developed is through a consensus process developed by NERC through industry with industry experts participating in the panel and with FERC staff members observing. Then the Commission takes the filing from NERC and then approves or directs changes.

This particular standard has been approved and is in effect. And, in fact, in January a new version of this standard has been approved and will become effective shortly. So from the standpoint of industry, as well as the experts at NERC and our staff review and the recommendations to the Commission and the Commission's determination, yes, it is enough.

Senator HOEVEN. Mr. Ott.

Mr. OTT. Yes, the requirements, certainly, I agree with Mr. Ortiz, is three years, but at PJM we test every year because we feel going above the standard is prudent in this particular case. At least in our region, we would test every year—or we do test every year.

Senator HOEVEN. Are you typical or atypical?

Mr. OTT. I'm not sure. I'd have to get back to you on that. I think my experience with the industry is people tend to exceed the standard. So I would think we're not alone.

Senator HOEVEN. Are there regulations that are an impediment or things that Congress could do that would be helpful in regard to this issue?

Mr. OTT. I think, in general, the blackstart, the controversy over blackstart is the expense, the cost of it. And there's been some controversy over the cost.

One other issue with blackstart is some of the emission rules in the emergency situation, getting relief from emission characteristics and rules is also something that we have to make sure we can streamline.

Senator HOEVEN. Ms. Ditto, you mentioned in your testimony that a Black Sky event, or a blackstart situation, would include the failure of not only our electric utilities but also our information and communication technology networks. Can you speak further about the importance of the communications aspect and how you deal with it?

Ms. DITTO. Yes, thank you, Senator, for the question.

As I mentioned in my testimony, utilities provide their own information and communications technology networks for the very reason that they need high levels of reliability. They need those communications networks to be available to them in restoration.

In a Black Sky, very serious situation, where we have a blackstart scenario, there could have been a cybersecurity event precipitating that. So utilities also have redundancy in their system to go to voice communications, as I mentioned earlier, and that's typically radio-based.

So they do have redundancy in their systems to deal with a cybersecurity attack. Will that get them everything that they need? Perhaps not, particularly given that there are policies being undertaken at the Federal Communications Commission around provision of those radio systems. You need radio spectrum to operate them and if you have interference during a restoration or a blackstart, you're not going to have the level of communications you need to enable those blackstart operations.

But we do maintain and manage our communications systems very well and we test them, and we also have fuel backup onsite for our communications systems, specifically.

Senator HOEVEN. That is tested at least once every three years?

Ms. DITTO. I'll have to get back to you for the record on how often we test our communications fuel backup systems, but we are vigilant in keeping those ready.

[The information referred to follows:]

U.S. Senate Committee on Energy and Natural Resources

October 11, 2018 Hearing

An Examination of Blackstart, the Process for Returning Energy to the Power Grid after a System-Wide Blackout, and Other System Restoration Plans in the Electric Utility Industry

Response from Ms. Joy Ditto to Question from Senator John Hoeven

Question: Senator Hoeven asked Ms. Ditto how frequently utilities test the generator and backup systems which utilities use to power their communications networks.

Response: Thank you for the opportunity to provide a written response to your question from the Senate Energy and Natural Resources Committee's October 11, 2018, hearing on the blackstart capabilities of electric utilities. As I understood your question, it was regarding how often utilities test the backup generation and battery backup for their private communications networks. I would like to provide you with the following answer to be included in the record for the above-referenced hearing.

As I mentioned during the hearing, electric utilities in most cases maintain their own private information and communications technology (ICT) networks. These networks are critical for managing day-to-day electricity reliability, resilience, emergency response, and to enable the use of intermittent resources like wind and solar or other distributed energy resources such that they do not cause power flow disruptions to either the Bulk Electric System (BES) or distributions systems. Utilities have been deploying these private communications networks for decades with reliability and coverage specifications that far exceed those of commercial networks deployed by telecommunications carriers. Because utility service territories can be vast and can cover varying topography, the geographic size of some of utility networks can rival those of many commercial carriers. These networks include wireline and wireless technologies, consisting of communications towers, receivers, and other network elements that allow utility workers to communicate in remote locations.

Because these telecommunications networks require power to operate, utilities back them up with different kinds of generation, depending on the location of the infrastructure, to ensure they remain operational during emergencies and power outages. Utilities typically use diesel generators and batteries to back up their communications systems, although the exact type of backup power varies from utility to utility.

While not uniform, all utilities have preventative maintenance programs for their entire communications networks, including the backup systems and generators needed to power these networks during emergencies. Importantly, utilities follow multiple federal and industry standards to ensure that their communications networks and devices—including the backup power systems supporting those networks—will function properly if the power from the grid is disrupted.

For example, the North American Electric Reliability Corporation (NERC) not only requires owners and operators of the BES to have redundant communications systems to operate in an emergency, the standards are specific about how those systems are to be tested. NERC Reliability Standard COM-001-3 at Requirement R9 states that, "Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall test its Alternative Interpersonal Communication capability at least once each calendar month. If the test is unsuccessful, the responsible entity shall initiate action to repair or designate a replacement Alternative Interpersonal Communication capability within 2 hours." Please see, https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=COM-001-3&title=Communications&jurisdiction=United States (emphasis added).

In addition, many utilities have interpreted NERC standard PRC-005-6, which deals with Protection System, Automatic Reclosing, and Sudden Pressure Relaying Maintenance and Testing (all functions essential to the reliability of the BES) to include utility communications networks if the communications networks would impact the reliability of the BES.

As was discussed during the hearing, most utilities test their systems much more frequently than required. Many UTC members monitor the generators—and battery back-up to that generation—powering their communications systems 24 hours a day, seven days a week. As part of this testing, utilities check to make sure the communications infrastructure has power and the ability to automatically switch to backup generation if needed.

Given how well utility communications systems have operated during the two most recent damaging hurricanes—Florence and Michael—I am confident that utilities take the necessary precautions to ensure their private networks will work during such catastrophic events. In fact, one of our members impacted by Hurricane Michael reported that despite the widespread power outages, their communications network—while it did sustain some damage—never lost core services for enabling restoration. This utility relied on the backup generators and battery systems at least initially during its response to the storm.

Please feel free to reach out to me or my staff should you have any additional questions. Thank you for your interest in these important issues.

Ms. DITTO. I'll give you an anecdote. After Hurricane Matthew a couple of years ago, we did ask our members if their communications systems stayed online and they did. We had electricity outages, but we did not have communications system outages for our own internal communications. The communications carriers were out. The telecommunications carriers were out of service. We stayed up. We did have to deploy backup power in some cases to our communications systems, but we were able to do that and they remained online.

Senator HOEVEN. But you would advocate that should be part of the test?

Ms. DITTO. Yes, I think we should have testing.

Senator HOEVEN. Mr. Galloway, in our state we are doing a lot with unmanned aerial systems, UAS, or drone development. We have a test site and a lot of other things and we have used them in situations where we have had storms, floods, various things. Talk about the role of UAS in terms of responding to a blackstart situation.

Mr. GALLOWAY. I think the role, the use of drones, is increasing very rapidly. It's turned out to be a very useful tool for normal operations like, kind of, overseeing rights-of-way in terms of vegetation management but increasingly in damage assessment.

Senator HOEVEN. Right.

Mr. GALLOWAY. So some of the incidents that I mentioned in terms of, like, restoration from Hurricane Irma, extensive use of drones, likewise Hurricane Harvey in the Houston area, extensive use of drones.

I do think that one of the issues that we need to look at is for any new technology like that, you have to protect that, again, from the cybersecurity standpoint, make sure that there's no issues.

And then lastly, I know that kind of coordination in terms of access to airspace post-event is an issue. Under Hurricane Florence, my understanding is there was a delay of restoration of up to a day just, kind of, coordinating access to airspace with first responders.

Senator HOEVEN. That is exactly right, and that is why utilities in our area are working with our UAS development efforts for some of those very reasons.

Thank you.

The CHAIRMAN. Thank you, Senator Hoeven.

Senator Smith.

Senator SMITH. Thank you, Madam Chair and Ranking Member Cantwell. I must be turning into even more of an energy nerd than I was before I got here because this is absolutely—it is really, really interesting. And thinking about all the different aspects of what we have to be addressing here in terms of workforce and startup energy sources and planning and testing and communications and also the research that we need. I mean, I think this is a very rich conversation.

I would like to focus in on the question of startup energy and, especially, how batteries could be helpful to this. This is something that I am quite interested in.

I introduced a bill last month that would fund energy storage capacity at the Department of Energy. This seems to me to be some-

thing that we can either be leading on in this country or following on, and I would rather have us be leading on it.

Mr. Torres, I might start with you and ask you a little bit about how you see battery storage as being an important component in the energy fuel source? I also have to say, I have been to La Junta and brought an ATV there with my dad. So it is a great community.

[Laughter.]

Mr. TORRES. Thank you for visiting.

[Laughter.]

Senator SMITH. You are welcome.

Mr. TORRES. So thank you for the question.

Energy storage, I think, can provide a bigger role, not just in blackstart, for the grid to increase resiliency overall. It can potentially provide a resource, maybe to help power up some of the smaller generators, to get those kick-started.

Senator SMITH. Right.

Mr. TORRES. It can also help with, you know, even smoothing some of that transition as we bring some of the various resources on. So there's a lot of opportunity in that particular space.

I think where some of the challenge is, is looking at how those systems work in conjunction, where energy storage works in conjunction with the various other technologies right now.

Senator SMITH. Is that an issue of having a coordinated response and making sure that the things are coordinated as they come back on?

Mr. TORRES. Absolutely, that's a big part of it. I think within blackstart, coordination is very, very important.

Senator SMITH. Yes.

Well, in Minnesota we get about 25 percent of our energy from wind and solar, and that is growing, not declining, so there are lots of reasons for us to care about battery research and advancing battery storage. This is an area where learning about how batteries could be helpful here strikes me as very important.

Would others on the panel like to comment about this?

Dr. Ortiz, I think in your testimony you talked about a utility in Southern California that was able to use battery storage to provide blackstart service.

Dr. ORTIZ. Yeah, as part of our review of the blackstart restoration plans with the participating utilities, staff identified one utility that had successfully used a battery for, in its blackstart procedures. And the reason for that is that a battery, of a certain size, is able to then provide the power that is required to startup a larger facility.

The process of blackstart is one of starting small and growing with a sequential pickup of both generation and load at the same time. So smaller scale resources that are more flexible tend to be those that are preferred for blackstart services. Batteries would fit into that category.

Senator SMITH. Would others like to comment on this?

Ms. DITTO. I would just say for, sort of, future facing, beyond blackstart, really when we're talking about a more modern grid and we're talking about edge of the grid issues, you need a high level of granularity for those storage facilities and for other vari-

able resources to work, needing storage, but also to interface with the electric grid for backup power. You need a high level of interaction and granularity to enable that because of the delicate balance between supply and demand on distribution grids.

So that's going to require even more communications technology to be overlaid.

Senator SMITH. Right.

Ms. DITTO. Which is going to pose some cybersecurity challenges and other challenges, but I think that's a key component to enabling these types of resources is the communications technology piece.

Senator SMITH. Very good.

Yes?

Mr. GALLOWAY. And then I would add to the extent that we are introducing more and more variable resources into the grid in terms of generation, that really does call for utility scale battery storage as part of the solution there.

Senator SMITH. Right.

It could be—just say a little bit more about that, what that would look like.

Mr. GALLOWAY. Well, I think we're talking today in the context of blackstart as Dr. Ortiz indicated when you start small and kind of grow but, you know, just the operating characteristics of a lot of the renewables are intermittent, right? And that introduces some added operational complexities.

So there's tremendous merit in being able to store that energy and bring it back online——

Senator SMITH. Right, right.

Mr. GALLOWAY. ——as necessary to, kind of, smooth out that intermittency.

Senator SMITH. So I would say that additional research and development around battery storage is useful in a variety of ways. It also could be very useful as we think about how to address blackstart challenges.

Mr. GALLOWAY. Correct.

Senator SMITH. Right. Great. Thank you very much.

The CHAIRMAN. Thank you.

Senator Hirono.

Senator HIRONO. Thank you, Madam Chair.

The advancements in battery storage are also very important for Hawaii, because I think we have the most ambitious sustainable energy goals—100 percent reliance on renewables by 2045. So battery storage is really important.

Ms. Ditto, first I would like to join you in commending the workers in the utility industry who do so much to restore power during and after a storm. We have so many storms these days. Right now, utility workers from across the nation are heading to Florida and other states affected by Hurricane Michael as part of the mutual agreements pre-established by utilities to help each other out after a disaster. I know that Hawaii utilities are grateful for the mutual aid agreements they have in place with their mainland counterparts, and they are just an example of the bonds that tie all Americans together.

Second, you noted the importance of electric utilities' private communications networks to ensuring recovery of the power system. As you no doubt remember, there were tragic instances of police and other first responders not being able to communicate with each other during the 9/11 attacks.

How well do different utilities' private communications systems operate with one another so that a utility crew from one company is able to communicate with utility workers say, in Hawaii or any other state recovering from a disaster? I am assuming, of course, that this kind of interoperability is really important for recovery efforts.

Ms. DITTO. Senator, thank you so much.

I just want to mention that I spent seventh grade through twelfth grade in Hawaii. I went to Punahou. So——

Senator HIRONO. Oh.

Ms. DITTO. I'm very familiar with the island and my family is still there so, yes, I just wanted to mention that. I miss being there sometimes.

I will say that that's a really great question, because this goes back to this idea of utility networks and utilities' reliance on wireless networks. In the case of radio spectrum, the available radio spectrum has not been dedicated to utility needs. So when you're in different spectrum bands you need to use different equipment and network devices. If you're in multiple bands, you cannot interoperate with each other. In some cases utilities in a geographic proximity to each other will share a band, but that is rare because of this lack of, sort of, dedicated spectrum. We're not necessarily asking for dedicated spectrum now because that ship has, kind of, sailed, but it does speak to the lack of being able to communicate.

I will say that in rare situations, we do share spectrum with first responders. That is something that could be excellent in the future. But again, the way policy has developed at the FCC has been not—there hasn't been a focus on critical infrastructure sectors. There's been more of a focus on commercial provision and telecommunication services. So this is an area that we'd like to, again, get the FERC and the FCC together around, but that interoperability does not exist today.

Senator HIRONO. Do you think it is important going forward for us to figure out how to do that?

Ms. DITTO. I think it would be incredibly important. I think the first step, again, is greater education about—radio spectrum, to be clear, is a finite resource and there are lots of demands on it.

Video streaming, I mean, all that we do at home, Netflix, all of that requires spectrum. So there are challenges, but we have to remind ourselves what is the priority. We all need electricity to exist in this modern world.

So, yes, we would like to see some changes in the future, but starting with some education of agencies would be great.

Senator HIRONO. Well, all these years after 9/11, I don't know if the interoperability issue has been resolved with regard to first responders. I did some work along those lines back then and my hope is that we're moving along, but you know, this situation creates yet another circumstance where we have to address those issues.

Mr. Torres, in May I was able to attend the opening of a biodiesel fuel power plant at the Schofield Army Barracks. This plant is the only blackstart-capable generator outside of the tsunami strike zone on Oahu and it was, kind of, astounding that a lot of these power plants are located close to where their fuel sources are, so they often are in tsunami zones. So they finally figured out that is not a good place to put power plants.

[Laughter.]

The 50-megawatt plant is owned and operated by Hawaiian Electric on land leased from the Army. In an emergency the Army can use the plant as part of a microgrid to provide secure emergency power to the Army Schofield Barracks' fuel stations, Kunia and Wheeler Army Airfield. This project can serve as an example to other military installations in need of a secure source of power.

I want to ask you, what opportunities and challenges do you see for broader use of microgrids for ensuring resilient power when the larger grid fails?

Mr. TORRES. That's a great question.

Microgrids are still maturing with regards to technology, with regards to procedures, with regards to standards but I think there is a tremendous opportunity, especially when you lose a transmission line where you may not be able to provide power from the bulk grid.

Especially when you have critical loads like a military installation or hospital or other government installations, you may want to add some resiliency with distributed resources at a microgrid level.

I think there's opportunity, as well, to explore how microgrids could provide blackstart capability to help start up the bigger grid. There's a lot of work that would still need to be done in that space from the regulatory perspective as well because, I believe, most of the regulatory guidelines for blackstart assume utilities are the ones that are actually putting the power on the grid and when you're talking about microgrids, you could have a whole spectrum, you know. In that case, you might have a military installation, essentially, operating from that perspective and putting power on the grid. So it would have to be very closely managed and controlled by a utility.

Senator HIRONO. If I may, Madam Chair?

Does the rest of the panel also agree that microgrids are an opportunity for us and we should be looking at how we can enable more microgrids?

Mr. OTT. Yes. In fact, we have seen microgrids actually provide restoration. For example, remember Hurricane Sandy and there were points of light in New Jersey that were microgrids and having them, actually, then look at a way to be a viable part of the picture in restoration. The real issue is coordination, visibility to operators like us.

So it's really—to work out those types of details, as the technology itself, we think, is probably a viable technology for blackstart. There's certainly promise there. We just need to do more.

The other issue is compensation. How are people going to be paid to help their neighbors? Because you can only depend on good neighbors so long, and then you need to systematically pay for it.

Senator HIRONO. Thank you.

Thank you, Madam Chair.

The CHAIRMAN. Thank you, Senator Hirono.

Senator Cortez Masto.

Senator CORTEZ MASTO. Thank you. Thank you, Madam Chair, and I appreciate the conversation.

I want to go back to what Senator Hirono was talking about, the interoperability. This, to me, is a big concern, not just because of being here in 2001, 9/11 happened, I was in Washington, DC. You could not use a cell phone.

After our horrific, horrific massacre, October 1, a year ago, my concern was the interoperability of our first responders and their access to the necessary communication and needs for public safety. I cannot stress enough that this is so important when we are addressing this issue, when we have a blackstart situation.

Ms. Ditto, you talked a little bit about the need to educate agencies. What do you mean by that?

Ms. DITTO. Yeah, so right now, I mean, the regulatory authority for radio spectrum resides primarily at the Federal Communications Commission which is outside of this Committee's jurisdiction. But because they have control over that radio spectrum, utilities weigh in with the FCC on their needs in this regard. But there's not a lot of understanding there.

Senator CORTEZ MASTO. Amongst the utilities?

Ms. DITTO. Amongst the FCC folks——

Senator CORTEZ MASTO. Okay.

Ms. DITTO. ——about energy needs and utility needs. And I would say that's true of other critical infrastructure providers as well. It's not their reason for being.

So our idea is let's get FERC and the FCC, because FERC has the jurisdiction over the bulk power system, get them together, get them learning from each other like FERC does with the Nuclear Regulatory Commission and then from FERC. And that could be a good place to start to have some of these more serious discussions about interoperability. But as we know, when you don't understand each other's perspective at all——

Senator CORTEZ MASTO. Right.

Ms. DITTO. ——especially in these very complex, I mean, these are very complex industries and I think having that, having technical conferences, having meetings, joint technical conferences, could be another thing that they do to educate each other or to educate the general public. There are a number of things that could be done to provide that education.

We could also, you could bring them up here and we could have briefings with Congressional staff and with members of the Senate and members of the House as well. There are a number of areas we could have this conversation, but I think before going to policy changes, that needs to be, we need to have that.

Senator CORTEZ MASTO. To have the conversation?

Ms. DITTO. Correct.

Senator CORTEZ MASTO. Mr. Ortiz, where is FERC with respect to this issue, and what are you looking to do after hearing the panelists and this discussion today?

Dr. ORTIZ. So FERC has engaged with other agencies in areas of mutual interest. Let me give you two examples.

The first is periodic meetings with both the FERC commissioners as well as the NRC commissioners on topics of mutual interest. The last meeting took place in June and covered the topics of resource adequacy and security.

And we just, the Commission, just recently signed and highlighted at our last Commission meeting a memorandum of understanding with the Pipeline and Hazardous Materials Safety Administration in order to further our mutual interest in that area.

I acknowledge that there are mutual interests here as well; however, as a FERC staff witness rather than a commissioner, I cannot speak on behalf of the Commission but I'd be happy to discuss this with the Chairman and then report back to the Committee.

Senator CORTEZ MASTO. I appreciate that and the need to engage the FCC. I mean, that is what I am hearing here. And it does not sound like that is happening yet——

Dr. ORTIZ. I can't say. The purview of my office is electric reliability, focused primarily on the development, implementation and enforcement of mandatory reliability standards.

There are some aspects, with respect to communications within our cybersecurity standards, but none at the level with respect to the actual provision of spectrum or appropriate bandwidth in order to facilitate such communications.

Senator CORTEZ MASTO. Thank you.

Mr. Ott, did you have anything to add to this? I just noticed you are shaking your head——

Mr. OTT. Well, yeah, the key is the electric sector, and I happen to chair on behalf of the Electric Sector Coordinating Council, the R&D Committee. One of those, one of the—in fact, the highest priority effort we have right now for 2018 and '19 is redundant communication and actually looking at technologies that would allow us to essentially, in a Black Sky scenario, stitch together whatever kinds of communications are available into a network that we could actually utilize.

And so, certainly from a utility perspective, we're not waiting for agencies to tell us what to do. We're actually trying to take action. I just thought that that might help with the conversation.

Senator CORTEZ MASTO. Okay, thank you. I appreciate that.

Actually, my time is up. Thank you so much for the discussion. Thank you, Madam Chair.

The CHAIRMAN. Thank you, Senator.

Senator King.

Senator KING. Thank you, Madam Chair.

I apologize to the witnesses for being late. There is no effort made whatsoever to coordinate schedules of hearings around here. I spent the morning in an Armed Services classified briefing which, believe me, you did not want to be in.

New England is enormously dependent on natural gas. I just looked at my little app from the ISO—74 percent of the power in New England right now is coming from natural gas.

In a polar vortex event or a pipeline disruption, a couple of questions: How would we fill in all of that power? And the second question is, I guess to the point of the hearing, can a gas plant

blackstart? Does it have the technical capability to restart and put power into the grid?

Mr. Ott.

Mr. OTT. Thank you, Senator King.

Yes, in fact, to answer your second question first, a gas unit can be blackstart. The key though is, obviously, if it can't get fuel——

Senator KING. Right.

Mr. OTT. Then we've got a problem——

Senator KING. Assuming it is a problem not of gas supply, but it is a problem somewhere on the——

Mr. OTT. Well, when you have a blackstart resource that has a single point of failure, meaning it could have an interruption of its fuel source and that would be a single point of failure, that's not a very robust blackstart resource because you want that blackstart resource to be there at all times.

Senator KING. Hydro could be though, couldn't it?

Mr. OTT. There we go, exactly. And that's the whole point, is diversity of supply. That same gas unit, by the way, could have liquid fuel backup onsite and certainly could then be more dependable.

But to answer your first question and this issue of—and certainly I'll talk to my colleagues in New England, Mr. Van Wheelie and others in New York, to try to coordinate our operations and our efforts, if you will, on resilience.

I think the key here, and we're about to put a study out on this issue of fuel security and what is the plan, if you will, if we become over-dependent upon gas.

In the PJM region, we're not quite as over-dependent as they are in New England, but the key is, what is the backup plan? How are we going to pay for liquid fuel, you know, delivery alternatives, when you have a gas infrastructure? In New England's case, what's the plan for depending on imports, other things like this? Those types of discussions on resilience are in the forefront right now. I think, certainly, our study will help.

Senator KING. I think you just answered my second question which is, should blackstart capability be part of any overall resource planning?

Mr. OTT. Yes.

Senator KING. A plan, and the answer is yes?

Mr. OTT. Yes.

Senator KING. I have to share a funny story. I was in college during the 1965 blackout. And in our college, we were all told never, ever plug in a hot plate. A fellow in one of our dorms plugged in a hot plate. The very moment he plugged it in, the lights went out.

[Laughter.]

He said, oh no, I've brought down the dorm. He walked outside. Somebody said the lights are out all over town. He said, oh no.

[Laughter.]

Then somebody drove by and said the lights are out all over the Northeast. And he said, now wait a damn minute.

[Laughter.]

So that is my 1965 blackout story.

How likely is this to happen? I mean, we have not had a major blackout of that nature for 50 years. Is this a realistic risk? Is it

something that should be on the top of our list or is this not as high a priority as, perhaps, other parts of grid security? Thoughts?

Mr. GALLOWAY. Well, we've been, in the transmission forum, spending a lot of time on the issue of resiliency under the assumption that however unlikely something of this scale could happen. And so, our planning has been, kind of, getting beyond design basis and assuming that the worst has happened for any number of different reasons and how would you, kind of, work back from that. So——

Senator KING. What are the reasons? Would this be a cyberattack or an explosion on a transmission system basis? What are we worried about here?

Mr. GALLOWAY. Well, we're looking at a couple of different things. One would be, as we're seeing in Hurricane Michael right now, there's natural effects, right? But you see an uptick in the number of, kind of, cyber phishing events, almost coincident with every type of natural occurrence like that.

Senator KING. Certainly, a cyberattack on the grid is a very serious concern.

Mr. GALLOWAY. That's probably the most serious concern right now and that in conjunction with some other kind of coordinated action or some natural event.

Senator KING. Thank you.

Mr. OTT. If I may, Senator.

The key is these very high-impact, low-probability events. I think we all, as a nation, are seeing these risks and risks that we haven't seen before. It used to be weather, you know, equipment failure. Now it's that plus intentional attack, cyberattack, et cetera.

The infrastructure of the nation, I think, the way we have to approach it though, by the way, this needs to be addressed. And I think the way we have to approach it is economically. We have to say yes, okay, let's take action, but let's take action that is well thought out, looks at all alternatives, doesn't focus on one answer, looks at diversity. I think the way the industry is approaching it, certainly the way PJM is approaching this, is to say, it is a realistic threat. Certainly we haven't seen it in the past, but the way to approach it is with thoughtful analytics, not panic.

I think you're seeing that. And I think, certainly from our perspective, we have and will propose to the regulators, here's a path forward that we think will work for everyone and certainly respect the fact that cost is, you know, you can't have unlimited expenditures here.

Senator KING. Right.

Mr. GALLOWAY. If I could, kind of, tag on to that very briefly? I echo everything Mr. Ott just said. So the term we use is, kind of, no regrets actions. We're really, we push on the concept really hard of taking a holistic approach and when you are working on resiliency issues, don't treat issues in isolation, right? Because economics is important and really, kind of, doing those things that would help you across a spectrum of a type of hazards would naturally be prioritized up on our list.

Senator KING. Madam, can I ask one more question?

The Northeast blacked out in 1965. The grid is much more integrated today than it was then in a lot of different ways. Is there

a danger that what happened in 1965, which was not a cyberattack but it was a series of successive failures, could spread nationwide, or are there gaps, are there protections?

Mr. OTT. Generally speaking, when you have one side of the system go down, you'll see a separation and you saw that in 2003 where we had some problems in Northern Ohio that took out New York into parts across there, but PJM system was able to stay up because of some strength of the transmission.

So it's likely that type of event is not going to take the system down globally. It's more, the global thing is more, in my opinion, more of an intentional attack type scenario and I think that's different. So, yes, for what it's worth, I believe the grid itself has some protections to stop blackouts from spreading too far.

Senator KING. Thank you.

Ms. DITTO. Well, also, there are three interconnections on the mainland U.S. and then, obviously, you have Alaska and Hawaii that have their own grids. But these interconnections are essentially islanded so, from a nationwide standpoint, it would be difficult to do. You'd have to have concerted, physical attacks in multiple locations throughout the U.S. and cyberattacks at the same time; otherwise, you could at least contain via interconnection, eastern, western or Texas.

Senator KING. Thank you.

I am delighted to hear that. I appreciate it.

Thank you, Madam Chair.

The CHAIRMAN. Thank you, Senator King.

This is one of those reminders that sometimes your geographic distance provides you a little bit of insulation. Oftentimes we feel very vulnerable and on our own with no neighbors to rely on, but when you do have a threat that could cross multiple systems, it is something where you say, okay, the attributes that whether it is microgrid, like Senator Hirono was talking about, or these very small grids that we would have, more independent grids that we have in Alaska, where you have almost greater resiliency because of how you are situated.

Senator Risch, do you want to hop in here?

Senator RISCH. I am going to pass, I have been chairing the Foreign Relations Committee.

The CHAIRMAN. I am sorry, sir.

We have had a fabulous discussion here this morning. So welcome.

Senator RISCH. Thank you.

The CHAIRMAN. The whole issue of no regrets and a policy, no regrets action, I think, is important and in your testimony you also, kind of, referred to this as a spare tire. You hope you never get that flat, but if you do, you have it in the car and you know how to use it. You have tested it or you have checked to make sure that there is at least air in it and you have a jack in there. So you are ready to go.

You are moving to this place where you do have greater comfort, in the sense that there is a diversification of fuel sources. You are doing more when it comes to the testing, the training, which is all important. But it seems to me, pretty clearly, the threats that are out there, as you said, Mr. Yardley, they are here, they are now.

I wonder if we are at that place where we need to help expedite this no regrets action plan a little bit more quickly.

The question to you, Mr. Galloway, is this a carrot or a stick? Is this something where FERC should look to imposing some standards or offer incentives to, kind of, move the utilities more quickly in improving their technology? I am curious about that. I also want to better understand when we are talking about the cost to the utilities, to the owners of these blackstart resources, we have talked a little bit about the cost, the carrying cost if you will, to have this standby service available.

Are these blackstart units, and I guess I will ask you, Mr. Ott, within PJM, are they adequately compensated? And what really is the cost of keeping this on, kind of, a hot standby, if you will, because you have a situation where you may need to be holding extra fuel. Is that the cost or is it the cost of installing better technology, better equipment?

Since we are, kind of, coming to the end of the discussion here today, I throw it out to you. I am curious to hear from you, Mr. Galloway, on what more needs to be done to get us to that better state of readiness and then the cost to do that.

Mr. GALLOWAY. So, if you look at, kind of, cyber threats as one of the primary challenges here, and I think we've, kind of, talked about that a number of different times, I'm not sure that more mandatory standards is the answer there.

The CHAIRMAN. Okay.

Mr. GALLOWAY. We're on version five of the Critical Infrastructure Protection Standards. That's a fairly heavy lift for a lot of the companies and may actually be a disincentive for folks declaring certain assets that are blackstart capable, as formal blackstart units, right, because of the carrying cost associated with the compliance. And then the other issues that you spoke to in observance of duel fuel capability and so forth.

So I think to Mr. Ott's earlier comments, if we see the need for, kind of, redundant, diverse, multiple fuel source, blackstart units, we want to make sure that there's a market incentive toward that, right? And that we approach it from a holistic, kind of, big picture view of are they appropriately, geographically distributed, right, from both a physical and an electrical perspective so that they plug into the system. I think PJM and others have done a lot of good analytical work on that, kind of looking at the sensitivity of moving to one fuel source.

So, perhaps, Mr. Ott would care to——

Mr. OTT. Yeah, and again, I didn't have this answer when Senator Manchin was here, but we do have actually 8,000 megawatts of blackstart in PJM, so it's probably even bigger than I thought.

But to answer your direct question, we have had several, and I say controversial, discussions with folks on both sides of the discussion on cost of blackstart. My opinion is we haven't done enough to make sure those resources are properly compensated. And certainly we are still, we are engaged in discussions to say the cost of having no single point of failure is not a small cost. It is a small number relative to the cost of electricity. It's probably less than one percent, probably even less than half a percent of the total.

But the point is it's an important contract if you want an important, I'll say guarantee, if you will, to the company to say, get rid of those single points of failure, spend some money to do it. It's money well spent, in my opinion. I think that it will be, this notion of resilience, if you will. To me, what resilience means as a system operator is I have degrees of freedom. I have margin for error. I have alternatives. And you never know, again, what situation you're going to be in, in these types of scenarios and having those degrees of freedom is invaluable. You can't go back and get it later after the events happen.

But I will say, frankly, what we really need, I think, is leadership from—I think we know what to do. Policy guidance from FERC, the FERC had put out a resilience NOPR some time ago, but there's been nothing since. Moving this policy guidance forward to say, let's engage in resilience, whether it be from a fuel security perspective or a system restoration. If you think about the pillars of resilience, the way I think about it, it's the power grid itself and making that as robust as possible and looking at these types of single point of failures.

There's the dependent systems like the natural gas infrastructure in looking at fuel security, and there's restoration and how you bring the system back should the other two not be sufficient. So, it's all those dimensions we need to address.

And really, this notion of resilience and bringing to the Floor, if you will, policy guidance from the regulator, is really what we need to get started on because it's been, we've been talking a little bit too long. We need some action on some of those things, especially this issue of fuel security and some other things we'll engage in conversation very soon on.

Ms. DITTO. I would just add that I think we're really at a crossroads in our sector. We have, as I think I mentioned in my testimony, expectations from our customers and from policymakers that we have a smart grid. We have a grid that's very efficient, that's flexible, that integrates intermittent resources, battery storage, other types of new technologies that are positive—electric vehicles. At the same time, those technologies, those communications technologies needed to enable those types of future facing grids leave us vulnerable on cybersecurity, right? So we have, I mean, we could go back to the dark ages and say, you know what, we don't want, we don't accept that risk. We don't want any cybersecurity risks, but I don't think we can put that genie back in the bottle, nor do I think we want to.

I think going forward what Andy mentioned about leadership, I think the leadership that you all could provide here is a better understanding from the technology side as well as from the communications side and the electric side, what our interdependencies are, where we don't have interdependencies, what policy issues, maybe, need to be addressed to enable us to provision these technologies and limit our cybersecurity risks.

And also, from a workforce standpoint, I would echo what Mr. Yardley said earlier, perhaps some additional funding, additional brainstorming around what we could do to encourage our workforce to get into these fields in the utility side as well as in the technology side.

So I think there are some things we could do to convene to really decrease stovepipes across industries, across the Federal Government so we can understand these vulnerabilities better. I think it is a good place to start in this crossroads time.

The CHAIRMAN. You had suggested earlier that you believe that the FERC and the FCC need to come together for these discussions. Does anybody know if that has ever happened?

Ms. DITTO. Again, I think maybe there's informal discussions that occur between the two agencies but to my knowledge, there's no formal venue for those discussions, at least in recent memory.

Mr. YARDLEY. Senator Murkowski, if I may?

The CHAIRMAN. Yes.

Mr. YARDLEY. Pulling on the thread of resiliency, we've talked a lot about fuel security, but echoing my statements earlier, cybersecurity is only one aspect of cyber resiliency. In our blackstart plans we have that same issue. Even if you have multiple fuel sources that are able to provide fuel to a given generation, you have that fuel security. You can't operate those generators unless you (a) have the people that are skilled to operate it, and (b) can rely on the technology, the control systems that are operating that grid, to function the way that they're supposed to, to run that generator to deliver that power where it needs to go, et cetera.

And that's also on the other side of it too. One thing that we have not touched on in blackstart is the delicate balance between the amount of power you generate and where that power goes. So you have to have loads that balance out the amount of generation. And that's also another attack factor. If somebody takes out large amounts of loads that are there, that throws that out of balance and you can have your crank path collapse.

The CHAIRMAN. Colleagues, any further questions or comments?

Well, I thank you all. This has been very informative and very worthwhile. I so value the expertise that we have assembled here.

I might close with just a little bit of a shout out to Alaska. Senator King just mentioned, who would have thought that it would actually be an advantage not to be on the broader grid? But it does require a level of innovation in a place like Alaska. We were quite pleased in May to be able to host National Lab Day up at the University of Alaska, Fairbanks. We had every one of our national labs represented there, so many of the directors. But it was great in the sense that we had all of these very learned people figuring that they were going to come and share with Alaskans all the great things that are happening and they learned so much from us because we just have to figure it out because when your grid is supplying, basically, a village of 350 people and you might be tied into another village a few miles separated by land, but not connected by road—pretty small, pretty high cost, how are you going to make this work? A lot of duct tape, a lot of ingenuity. I think it is important that we all recognize that we can learn so much from the way that we are situated differently around the country.

So we have our own fair share of experts up there and would certainly welcome those who want to come together to collaborate.

A very important issue this morning and just some good resources. I am intrigued by what you have stated, Ms. Ditto, that we need to be breaking down more of these silos within these agen-

cies and within those who are working on these very important issues and make sure that there is better communication, better understanding and a more unified strategy going forward because, as you point out, Mr. Yardley, we are here, it is happening now.

With that, the Committee stands adjourned.

[Whereupon, at 11:59 a.m. the hearing was adjourned.]

APPENDIX MATERIAL SUBMITTED

Questions from Chairman Lisa Murkowski
Committee on Energy and Natural Resources

For Dr. David Ortiz
Acting Director
Office of Reliability
Federal Energy Regulatory Commission

Question 1: *The joint report by FERC and NERC suggested that utilities should engage in more realistic and frequent testing of their blackstart plans.*

- *What can expanded testing of blackstart resources teach our grid operators about their ability to recover from a widespread blackout?*

Answer: Expanded testing of blackstart plans executes specific steps of the system restoration process. Specifically, it involves energizing an entire cranking path as would be needed to recover from an actual blackout. Thus, it provides additional insight into and validation of a utility's system restoration plan and its readiness to execute its system restoration plan. Such insight may not be achieved through computer simulations or tabletop exercises. The nine utilities that were part of the Blackstart Resources Availability Study (BRAv) used the knowledge gained from expanded testing by incorporating it into system restoration drills and system operator training.

- *What are some of the roadblocks to expanded testing of our blackstart resources? Are these operational, regulatory or financial?*

Answer: Some obstacles the BRAv study identified to expanded testing of blackstart capability are listed below. They include operational, regulatory and financial issues:

1. Customer interruptions (Operational) – Expanded testing frequently involves the need to de-energize or interrupt certain parts of the bulk electric system, meaning that some customers would experience service outages for a period of time while the test is performed. One specific challenge is scheduling these outages. Moreover, the affected commercial or industrial customers might request compensation for any scheduled interruption in their electric services. For these reasons, the joint report recommended that utilities take advantage of planned outages to perform expanded testing of blackstart plans to the extent possible.

2. Coordination among parties (Operational) - Successful expanded testing requires extensive coordination among utilities. To perform these tests without loss of load, utilities must coordinate with all affected parties, including the blackstart and next-start generator operators, the transmission owner, the transmission operator, and in some cases the reliability coordinator. This coordination includes how to mitigate the next-start generating unit's startup risks under test conditions. This coordination also includes arranging a schedule for testing to minimize any associated cost and reliability impact

(e.g., by running the test when the blackstart generating unit is offline, the next-start generating unit is offline, and system loads are at a lower level).

3. Emissions limits (Regulatory) - In some regions, registered entities have to abide by strict state and local emissions regulations for some of their blackstart units (whether during normal operations or during any operations required for blackstart testing), and these operating limits are more likely to be reached during expanded blackstart testing. These emissions restrictions effectively limit allowable run hours during a 12-month period, and could preclude additional or expanded blackstart testing, absent appropriate permits or waivers.

4. Cooperation of next-start generating unit owners (Financial) - Expanded testing requires the cooperation and involvement of the next-start generating unit owner. In some cases, next-start generating unit owners hesitate to operate their generating units as blackstart units because of lost revenue from being offline to participate in the test, the risk of damage to their units, and the lack of a mechanism (market or otherwise) to provide compensation for any such damage should it occur.

   • *Does the federal government need to provide more of an incentive for expanded testing of blackstart resources?*

Answer: Whether such an incentive is needed is not yet clear. The BRAv study report recommended a study of the adequacy of compensation for blackstart and other resources supporting system restoration including expanded testing. Specifically, the report recommended "that Regional Transmission Organizations (RTO), Independent System Operators (ISO), or other appropriate entities consider an examination of the adequacy of compensation for services and benefits provided by blackstart resources, including any potential threat or impact on blackstart resource procurement and retention under current compensation mechanisms" (BRAv Study Report at 2-3). The outcome of such a study would inform a discussion of the need for incentives to alleviate utilities' operational, regulatory and financial risks pertaining to expanded testing.

Question 2: *Dr. Ortiz, to what extent have you personally communicated with staff at the Federal Communications Commission concerning the need for adequate communications in operating the power grid?*

Answer: As of November 7, 2018, I have not had any personal communications with staff at the Federal Communications Commission.

U.S. Senate Committee on Energy and Natural Resources
October 11, 2018 Hearing
An Examination of Blackstart, the Process for Returning Energy to the Power Grid after a System-Wide Blackout, and Other System Restoration Plans in the Electric Utility Industry
Questions for the Record Submitted to Mr. Andrew Ott

Questions from Senator Mazie K. Hirono

Question 1: In your testimony you state that "we need to ensure the grid is resilient to extreme but plausible events and need to decide the degree of resilience investment that is reasonable for the ratepayers of the region to bear. The ratepayers of our region, be they households or businesses, shouldn't be responsible for securing the grid from a World War III type of attack. At some point, that becomes the task of national defense, paid for by taxpayers across the land."

This statement seems to conceive of resilience as being about securing the existing electric grid and would seem to place the final burden of responsibility on national defense. It seems to sidestep the fragility of the existing electric grid to attacks and extreme weather events. Shouldn't we be asking how to better use taxpayers' and utility customers' dollars toward building a smarter, more flexible, adaptable, and cost-effective electric grid, rather than simply securing what already exists?

We definitely should be asking how to better use taxpayers' and utility customers' dollars toward building a smarter, more flexible, adaptable, and cost-effective electric grid. This includes looking for cost effective and innovative approaches at both the transmission and distribution level to include innovations in market signals to incent more efficient resources as well as innovations in approaches to transmission planning. In some cases, upgrades to the existing infrastructure and the installation of new equipment such as Phasor Measurement Units can improve the efficiencies of existing transmission facilities. In other cases, new investment can be directed at storage devices, demand response, distributed energy resources, renewables, and microgrids. All of these investments should be made with customer reliability and cost efficiency in mind.

My reference to a "World War III type of attack" was merely to point out that although there is much that can and needs to be done in the individual regions and among the individual grid owners and operators, there is a policy question to be discussed as to where the responsibility of individual grid owners and operators to ensure that the grid is sufficiently resilient to attack begins and ends and where it transforms over to activities which are more in the nature of protecting our homeland through national defense and homeland security strategies. There is no clear demarcation point on this continuum. My main point was to tee up this issue and indicate that as part of the resilience discussions going on at FERC and elsewhere, these points on the continuum will need to be better identified and discussed to ensure a cohesive national grid resilience policy across the nation.

Question 2: If you had the opportunity to rebuild the electric grid today with a resilience strategy in mind, what would you do differently?

Today's grid was built over an extended time period. As a result, the grid was largely designed for one-way delivery of power from large central station generators to load centers in major population areas. As a result of advances in technology, the development of competitive wholesale electricity markets and more coordinated operation of the grid by large Regional Transmission

U.S. Senate Committee on Energy and Natural Resources
October 11, 2018 Hearing
An Examination of Blackstart, the Process for Returning Energy to the Power Grid after a System-Wide Blackout, and Other System Restoration Plans in the Electric Utility Industry
Questions for the Record Submitted to Mr. Andrew Ott

organizations we have been able to use that original design more efficiently so as to facilitate the flow of power from new locations such as wind farms atop mountain ridges to a more diverse set of loads. Moreover, grid development today is limited by the scarcity of new right of way in our urban and suburban areas and overall public opposition to the siting of new transmission lines. These constraints force the industry to continue to find ways to drive additional efficiencies within the original grid configuration.

By contrast, were we to start with a blank sheet of paper and design the grid today, we would site new transmission lines in locations that would reach additional sites where renewable generation is likely to develop and build in capacity to recognize the needs of electric-intensive loads such as data centers as well as the phenomenon of urban sprawl. We would further build into our new grid design additional redundancies in grid configuration to ensure that the grid is resilient to withstand potential physical and cybersecurity incidents. Finally, we would design the grid to further capitalize on the movement toward micro-grids and distributed generation.

The key difference in approach is that rather than *adapting* today's grid to meet these new challenges (which, to date we have been able to do quite successfully despite the original grid configuration dating back in many cases over decades), we would be able to start with a new configuration that would incorporate these additional requirements from the original design phase.

The costs of such an entire redesign and the challenges in siting an entirely new grid configuration make this path implausible in the near term. Nevertheless, we continue to work to reconfigure and advance today's grid to meet future challenges and remain committed to continuing to do so in the future.

U.S. Senate Committee on Energy and Natural Resources
October 11, 2018 Hearing
An Examination of Blackstart, the Process for Returning Energy to the Power Grid after a System-Wide Blackout, and Other System Restoration Plans in the Electric Utility Industry
Questions for the Record Submitted to Mr. Juan J. Torres

Questions from Senator Mazie K. Hirono

Question 1: I thank NREL for its assistance over the years to Hawaii's effort to transition to 100 percent renewable power by 2045. In your testimony you mention NREL's recent project with Hawaiian Electric and other partners to evaluate how distributed energy resources could help restore grid stability. What lessons did NREL learn from the project that could benefit Hawaii and the rest of the country? How does NREL plan to build on the results of the grid stability project in terms of future research projects, recommendations to stakeholders, or other steps?

Answer 1: It has been a pleasure to work with Hawaiian Electric and the other stakeholders towards Hawai'i's ambitious energy goals. It became clear through our Grid Modernization Laboratory Consortium (GMLC) project and through other projects in Hawai'i that each stakeholder has strongly-held beliefs about how best to reach the 2045 goal. Partly because of geographical limitations and partly because of enthusiasm for locally-sourced energy, a large portion of the electrical energy in Hawai'i already comes from distributed energy resources such as solar photovoltaics, largely owned by individual citizens, and that portion is expected to continue to grow. This poses a mix of interrelated technical and policy challenges that can only be addressed by bring together all of the relevant stakeholders. We are honored to have been part of the stakeholder discussions leading to a consensus agreement, which concluded that requiring certain smart inverter functionality in Hawai'i would be in the best interest not just of the utility, but of the distributed energy resource industry and the community at large.

As a national leader in the high penetration of distributed energy resource resources, Hawai'i is identifying and addressing integration challenges that many other states will soon face, so we see Hawai'i as a "postcard from the future" that the rest of the country can learn from. In fact, one of the key outcomes of our GMLC project was to provide technical input to the national standard for interconnection of distributed energy resources (IEEE Standard 1547), which just completed a major NREL-led revision in April of this year. Specifically, the Hawai'i GMLC project results convinced IEEE 1547 stakeholders to allow distributed energy resources to provide very fast (sub-second response time) services to help stabilize the grid following major events such as the loss of a large power station or transmission line. While such fast grid frequency stabilization from distributed energy resources may not be needed today in most of the mainland U.S., ensuring that the smart inverters sold today are *capable* of it is one step towards positioning the nation's electric grid for increased resilience and avoiding extremely costly retrofits in the future. Indeed, the impact of distributed energy resources, such as solar, on grid stability has emerged as an important issue in the power systems community today. Smart inverter stability services such as what the Hawai'i GMLC project recommended (and the Hawai'i Public Utilities Commission approved) are one way of helping distributed energy resources be part of the solution.

NREL, Hawaiian Electric, and other stakeholders have discussed a number of possible future research projects that would continue the significant progress made by the Hawai'i GMLC project. For example, as the power system continues to evolve such that more and more generation comes

U.S. Senate Committee on Energy and Natural Resources
October 11, 2018 Hearing
An Examination of Blackstart, the Process for Returning Energy to the Power Grid after a System-Wide Blackout, and Other System Restoration Plans in the Electric Utility Industry
Questions for the Record Submitted to Mr. Juan J. Torres

from inverter-based resources, such as solar and batteries, those resources will need to assist with many more of the grid-stabilizing tasks that are largely performed by rotating generators today. Future research is needed to address unresolved issues, including:

- How should inverters best be designed and controlled to operate more synergistically with conventional rotating machines to ensure grid stability and resilience to disturbances, and what auxiliary technologies may be needed as the portion of electricity produced from these new sources grows?
- How will power system protection technologies that ensure grid resilience to faults need to be updated as the grid evolves to include higher penetration of distributed energy resources?
- As the grid comes to depend on inverter-based generation for reliability and resilience, how can we ensure that the largely software-defined behavior of these devices performs up to the expectations of grid operators?
- What control architectures can best leverage distributed energy resources to increase grid reliability and resilience?

We would like to thank Hawaiian Electric and the state of Hawai'i for allowing NREL to help you meet your energy goals.

Question 2: If you had the opportunity to rebuild the electric grid today with a resilience strategy in mind, what would you do differently?

Answer 2:
If we had the opportunity to rebuild the electric grid today, we would base the new grid on an *Autonomous Energy Grids*[1] framework. Similar to autonomous vehicles—which do not require a physical driver and can make decisions on how to most effectively transport a person from one place to another—Autonomous Energy Grids (AEGs) do not require physical operators, would be extremely secure and resilient (self-healing), and would self-optimize in real time to ensure economic and reliable performance while integrating energy in all forms. To achieve these goals, Autonomous Energy Grids rely on scalable cellular blocks that can self-optimize when isolated from a larger grid and participate in optimal operation when interconnected to a larger grid. These scalable cells can be areas of the grid that can run independently as microgrids or be parts of the grid that are segregated from a control perspective. Although they do not have enough local generation to carry the full load of the cell, they could support critical loads when separated from the larger grid. The Autonomous Energy Grid concept allows for the use of optimization and

[1] "Autonomous Energy Grids", B. Kroposki, E. Dall'Anese, A. Bernstein, Y. Zhang, and B. Hodge, *Hawaii International Conference on System Sciences, Waikoloa, Hawaii, January 3–6, 2018* https://scholarspace.manoa.hawaii.edu/bitstream/10125/50229/1/paper0342.pdf

control across cells in cases when the cells can form independent microgrids and when they can control assets but not intentionally island.

The key features of Autonomous Energy Grids include:

- **Autonomous** – Makes decisions without operators.
- **Resilient** – Self-reconfiguring, cellular building blocks with plug-and-play capability, able to operate with and without communications between devices and system operators, and robust to communication interruptions and data asynchronies.
- **Secure** – Incorporates cyber and physical security against threats, eliminates single points of failure, reduces system vulnerability to cyber-physical attacks.
- **Reliable and Affordable** – Online self-optimization of power flow subject to stochasticity of variable renewable energy sources for both economics and reliability
- **Flexible** – Able to accommodate energy in all forms including coal, natural gas, nuclear, hydro, and variable renewables; support integrated coordination between grid assets and edge resources.
- **Situation Awareness** – Distributed online state estimation to achieve high system observability with measurements that may be inaccurate and spatially- and temporally-sparse
- **Intelligent** – Adjust grid operation proactively in response to situation awareness outcomes and predictions; able to seamlessly transition between grid-connected and islanded operations.

Other key elements that we believe are important in framing a path for the future grid are the business models, regulatory structures, and policies that enable optimized use of the grid. Unless all of these align with the grid capabilities, we will not be able to take full advantage of investments we make in the grid.

These concepts build upon the work currently funded under the Department of Energy's Grid Modernization Initiative (GMI), but we advance the operating paradigm to a state where minimal human intervention is required to manage the grid. Even though we do not really have the ability to rebuild the electrical grid from scratch, we feel we can develop a path from the current grid to the grid of the future that we envision.

U.S. Senate Committee on Energy and Natural Resources
October 11, 2018 Hearing
An Examination of Blackstart, the Process for Returning Energy to the Power Grid after a System-Wide Blackout, and Other System Restoration Plans in the Electric Utility Industry
Questions for the Record Submitted to Mr. Thomas J. Galloway, Sr.

Questions from Chairman Lisa Murkowski

Question 1: The joint report by FERC and NERC suggested that utilities should engage in more realistic and frequent testing of their blackstart plans.

a. What can expanded testing of blackstart resources teach our grid operators about their ability to recover from a widespread blackout?

Expanded testing of Blackstart Resources[1] can inform grid operators about valuable aspects of blackstart restoration, such as verification of plan details, communications, model validation, and assurance of required operating characteristics. Specifically, expanded testing allows entities to test the units' ability to produce, monitor, and control system characteristics (e.g., voltage and frequency) during early stages of the restoration and help entities obtain a better understanding of the actual timing to complete this initial stage of the restoration process. However, grid operators must be prudent when pursuing expanded testing and only attempt when the benefits outweigh any inherent risks to reliability (i.e., the system needs to be placed in off-normal configurations during testing) and the additional costs that would be incurred.

b. What are some of the roadblocks to expanded testing of our blackstart resources? Are these operational, regulatory or financial?

Increased testing involves a number of potential roadblocks, including operational, regulatory, and financial, some of which are highlighted in the FERC-NERC-Regional Entity Report.[2]

Testing results in increased costs, and there is currently a lack of mechanisms (market or otherwise) to compensate generation owners for this activity.

Many generation owners operate under constrained emissions requirements, which may impede the ability to perform expanded testing.

In addition, operational complexities can be encountered performing expanded testing, including the need to place the system in off-normal configurations. In many cases, entities must de-energize or interrupt certain parts of their system in order to perform expanded testing. Additional coordination is required among the participants, which may include transmission and distribution owners and operators, generation owners and operators, affected customers, and the Reliability Coordinator. This coordination also requires scheduling the tests to minimize any associated cost and reliability impacts.

[1] Blackstart Resource definition can be found in the Glossary of Terms Used in the NERC Reliability Standards.
[2] FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans – Recommended Study: Blackstart Resources Availability. See page 41-43.

U.S. Senate Committee on Energy and Natural Resources
October 11, 2018 Hearing
An Examination of Blackstart, the Process for Returning Energy to the Power Grid after a System-Wide Blackout, and Other System Restoration Plans in the Electric Utility Industry
Questions for the Record Submitted to Mr. Thomas J. Galloway, Sr.

Regarding operational complexities, the North American Transmission Forum (NATF) can support its members that encounter obstacles when considering expanded testing. The NATF is built on the principle that timely and detailed information sharing among members is key to improving the reliability and resiliency of the transmission system. As such, the experiences and lessons learned of one member are shared through the exchange of operating experiences and NATF workshops.

In areas in which expanded testing is not performed or not feasible, simulation technology, which has advanced over the years, allows entities to better replicate actual system conditions during a blackstart training scenario. In these instances, NATF facilitates the sharing of best simulation techniques through its practice groups.

c. Does the Federal Government need to provide more of an incentive for expanded testing of blackstart resources?

A combination of government and industry actions can strike the right balance to provide incentives for expanded testing of Blackstart Resources. Currently, some mechanisms are in place to promote the expanded testing. While the NERC Reliability Standards do not require expanded testing to realize the aforementioned benefits, many entities perform this testing, where feasible. The NATF provides several venues for members that exercise expanded testing to share best practices and lessons learned with other members.

The Federal Energy Regulatory Commission has the authority to rule on proceedings that could determine vehicles to compensate entities for the risks they may incur during expanded testing. Research and projects currently being performed by the Department of Defense and the Department of Energy, as highlighted in the testimonies of myself and Mr. Torres, provide examples of the public-private partnerships to improve the overall ability for the grid to return to service from a blackstart scenario.

Question 2: If a blackstart event is the result of a cyberattack or other attack, our military could be tasked by the President with taking some sort of appropriate action against those who attacked us.

a. What is the role of the electricity industry in an attack? Is it purely defensive?

The role of the industry is partially defined by the NERC Critical Infrastructure Protection (CIP) standards. These standards require applicable entities, among other things, to have cyber security incident response[3] and recovery[4] plans, as well as physical security[5] plans. These plans are developed and implemented such that the entities are best equipped to identify, classify, and

[3] CIP-008-5 - Cyber Security - Incident Reporting and Response Planning
[4] CIP-009-6 - Cyber Security - Recovery Plans for BES Cyber Systems
[5] CIP-014-2 - Physical Security

respond to cyber and physical incidents. The general industry posture is to maintain a defense-in-depth approach to attacks, not to retaliate in cyber or physical warfare.

As stated in my testimony, many efforts are being taken by the industry to prepare for an attack. These include transmission system hardening, spare-parts procurement, mutual aid programs, NATF Supplemental Operating Strategies[6], and education and information sharing (e.g., NATF/EPRI Resiliency Summits). Further, drills and exercises are performed to simulate attacks and practice industry response and recovery; examples include the NERC GridEx and the DOE Liberty Eclipse exercises. During these exercises, electric industry entities—along with federal and state agencies, law enforcement, and other critical infrastructure participants—simulate advanced persistent cyber and/or physical attacks that target the grid. These activities allow the players to exercise incident response plans, engage critical interdependencies, and improve communications, including information sharing. An important aspect to thwarting attacks is to enable a secure line of communication between the government and industry to share intelligence that is both useful and actionable.

b. In the event of an attack on our grid, can the electric industry ensure that the military is adequately supplied with electricity so that the military can respond to the attack? Or is it the responsibility of the military to ensure that it can operate without electricity service coming from civilian infrastructure?

It is the mission of the electric industry to serve its customers in a safe, reliable, and economic manner. However, it is not practical to assume that can be done 100% of the time. The transmission and distribution grids cannot reasonably be planned and operated to withstand every catastrophic event, whether natural or man-made.

Blackstart Resources are not designed or intended to provide the national security infrastructure or military installations a constant electricity supply. In response to a high impact, low frequency event that causes a partial or full loss of the grid, utilities define their load restoration priorities as part of their restoration plans. It is imperative for the owners of the key facilities to communicate with their local power supplier to understand each other's needs and priorities before and during a restoration event. However, it is incumbent upon utility customers to prepare for the possibility to cope for a duration of time until power can be restored.

Onsite power should be installed at key facilities and tested on a periodic basis. Further, careful consideration should be given for a fuel-procurement strategy that allows critical facilities to cope with a long-duration outage (e.g., an outage due to catastrophic physical damage).

[6] Bulk Electric Systems Operations absent Energy Management System and Supervisory Control and Data Acquisition Capabilities - a Spare Tire Approach

U.S. Senate Committee on Energy and Natural Resources
October 11, 2018 Hearing
An Examination of Blackstart, the Process for Returning Energy to the Power Grid after a System-Wide Blackout, and Other System Restoration Plans in the Electric Utility Industry
Questions for the Record Submitted to Timothy M. Yardley

Questions from Chairman Lisa Murkowski

Question 1: The security of third-party vendors who sell their power grid equipment has received some attention. FERC has already acted to require a NERC standard on third-party vendors. In addition, Bloomberg has recently published news stories raising the possibility that China has inserted miniature chips into hardware for the purpose of enabling cyberattacks.

- Recognizing the complexity of the blackstart process, how confident are you in the security of the hardware that is needed for system restoration?

- What actions are being taken by both government and industry to ensure that the hardware of the grid is adequately protected? Are those actions sufficient?

Answer 1:

While the security features and protections implemented in vendors' equipment have increased, in many cases, devices still have not been hardened sufficiently to prevent tampering by a determined adversary. The methodology and frequency of such attacks have advanced greatly over recent years. More importantly, though, it is nearly impossible to state a confidence level in the security of particular hardware without two important things: 1) an evaluative metric by which to quantify a claimed confidence level in terms of a particular threat, and 2) a method by which to verify and validate such claims or protections. Item 1 is an area of current research and much debate. Item 2 is twofold, encompassing 1) the need for a capability to securely access devices to assess their security and functionality down to the lowest levels that cannot be tampered with, and 2) a facility (testbed environment) and toolset that can assess individual devices and compare findings against a known ground truth. There are other complexities in getting ground truth, but they would require a longer and more technical discussion. Neither of these items is a solved problem, and both need more focus.

Thankfully, much research is being done to explore the quantification and assessment of security at both the academic/national lab level and the government/industry level. These efforts are generally referred to under the moniker "the science of security." In addition, programs like the DARPA RADICS effort are looking at developing both an assessment methodology and toolsets to enable security assessment of devices, but that work is still in progress, and as a nation, we need more focus on pursuing such efforts more broadly. There is also prior and current research focused on creating tamper-hardened or secure devices, leveraging techniques like cumulative attestation, as an example. These technologies allow us to understand definitively whether the firmware integrity of a device has been compromised in some way. Regardless of the solution space, the reality is that much of the operational gear in the field does not have these features and relies on physical and cyber perimeter protection as their critical line of defense. That reliance on a perimeter is mostly a fallacy when faced with a determined adversary. While actions are being taken, they are not yet sufficient, nor are they sufficiently present in the deployed systems.

U.S. Senate Committee on Energy and Natural Resources
October 11, 2018 Hearing
An Examination of Blackstart, the Process for Returning Energy to the Power Grid after a System-Wide Blackout, and Other System Restoration Plans in the Electric Utility Industry
Questions for the Record Submitted to Timothy M. Yardley

However, there is a missing piece in the puzzle that can be solved. Protection of devices is critically important, and I discussed the state of that effort in my testimony. I keyed in on the concept of resiliency, which reflects the realization that such protections will eventually fail. The process of restoration after those protections fail has previously received insufficient focus, outside the current RADICS program. Currently, vendors are the only entities that can restore a device that has been tampered with. That is a workable approach when there are available resources in stock or on hand, as any tampered-with gear is simply replaced with on-hand items. However, in the face of a blackstart caused by a cyber attack with wide-reaching cyber "damage", it is plausible that resources would be exhausted and devices could not be recovered via traditional means, as seen in the Ukraine. Such a situation would require deeper remediation and access than what is typically available. A large-scale attack would also likely exhaust the supply and the ability of the vendor to repair or replace devices expediently. This means that people other than the device manufacturers need to be able to assess devices' security and restore them and we need to develop interfaces and toolsets that facilitate this. That also implies a deeper level of access to the physical devices than what can currently be obtained—and it would need to be possible to securely unlock that access when necessary.

Question 2: You testified that: "We need to focus on increasing the capabilities of our people as much, if not more, than we focus on our technology."

- What are some of the best ways to start focusing on training people? Is it university education? Or training at the utility?
- Who needs to be trained? Is it the operators in the control room? The cybersecurity experts? The linemen and linewomen out in the field?

Answer 2:

Traditional cyber security is a cat-and-mouse game. The adversary only needs to find a single mistake that the defender has made, so it is inevitable that a compromise will happen. My statement about needing to go beyond cyber security and focus on resilience rings true in workforce development as much as it does in technology. We must be resilient, and we must acknowledge that at some point we will fail. With that said, we must educate at multiple levels to be prepared for these failures. We must create a strong pipeline of workers who have not just cyber security awareness, but deeper understanding and actionable skills. While that pipeline could be cemented in university education, as a nation we must think more broadly. We should work to encourage and nurture interest in these topics beginning with early childhood education, much as we have been advancing STEM education more broadly. We should grow and refine that interest in primary, secondary, and tertiary education and ultimately on the job as well. We should also focus on refreshing our existing workforce with the emerging cyber security skills of today, building on their wealth of existing knowledge.

We have to adapt. We have an existing workforce that needs to understand new technologies, build skills, and incorporate that body of knowledge into their daily work. That process has been assigned many

U.S. Senate Committee on Energy and Natural Resources
October 11, 2018 Hearing
An Examination of Blackstart, the Process for Returning Energy to the Power Grid after a System-Wide Blackout, and Other System Restoration Plans in the Electric Utility Industry
Questions for the Record Submitted to Timothy M. Yardley

different labels, such as "re-skilling," "revitalizing," "refreshing," and "professionally educating," among many others. The label doesn't matter as much as the concept. We have existing people that need to be effectively and efficiently equipped to understand and evolve in the face of increasing cyber security threats.

To go back to my testimony, we are only as strong as our weakest link, and, from a cyber security perspective, that is often our people. To err is human, and one mistake may be enough to enable adversaries to accomplish their goal, so we all need to be cognizant of this and diligent in building systems, processes, and people that are resilient to help detect and respond to threats. Each level of education has a role in increasing the depth and breadth of our talent pool. To reference Bloom's Taxonomy, everyone needs to remember the tenets of cyber security and recognize when they may be jeopardized. Some subset of those people need to understand what the compromise of those tenets means, and some further subset needs to be able to apply the protection concepts that can address those impacts. Beyond that, we need people who can then analyze and evaluate information to develop a more comprehensive response or future defense. Ultimately, we need to create new approaches to building more resilient systems. By working together on people, from children all the way through retirees, we can address that need across the board. As we go deeper in the level of knowledge and understanding, the pipeline funnel will, of course, narrow; we must be cognizant of that and create a large enough base to make sure we achieve the depth of talent necessary.

Training needs to happen at every level, both horizontally and vertically. Vertically, it needs to go from the top (the boardroom) to the bottom (employees in the field). Horizontally, it needs to address organizational impact covering non-operational roles, such as legal, contracting, marketing, and HR, to name a few. Any path is a potential foothold for an adversary who wishes to use it to his or her advantage; therefore, every person potentially plays a role.

Questions from Senator Tammy Duckworth

Question 1: Scientists warn that extreme weather events are becoming more frequent and severe because of climate change. Failure to invest in infrastructure maintenance and fund critical upgrades forces Illinoisans to rely on unreliable legacy systems that should have been decommissioned years ago. That is why we must have the policies and technology to strengthen our grids resiliency and security.

In your testimony, you discuss the importance of developing a testbed environment where researchers can ensure we have the mission-critical tools to blackstart the electric grid. What types of investments do we need to make to get a testbed up and running?

Answer 1:

Thankfully, Illinois already has a strong start on this with the University of Illinois at Urbana-Champaign's CEER Testbed, which I envisioned a decade ago and built. That facility is able to interface with the Ameren Technology Application Center (TAC) that was built to support the investigation of emerging technologies

U.S. Senate Committee on Energy and Natural Resources
October 11, 2018 Hearing
An Examination of Blackstart, the Process for Returning Energy to the Power Grid after a System-Wide Blackout, and Other System Restoration Plans in the Electric Utility Industry
Questions for the Record Submitted to Timothy M. Yardley

and their application to the Ameren power system. A significant amount of investment is still needed, however. The Illinois testbed is great, but its operational aspects must be transitioned to other partners and distributed throughout the nation in order to scale to a national level. While it would be great if everyone could come to Illinois to use the facility, the reality is that it would be nearly impossible to scale and meet the demand with just one facility or one central location. This is not a negative, but an opportunity. Every region could have a facility that provides the needed capabilities and is tailored to the operations of the critical infrastructure in that region. What I have built with portable testbed environments under the RADICS program could be an excellent first step towards providing such capabilities throughout the nation. In order for that vision to be realized, there needs to be a transition partner to spearhead the effort that also has the desire to use it once in place and supported by the necessary funding with which to build and maintain it. The portable environments that I mentioned would provide a great basis to build upon for national distribution of the above types of capabilities. More investment, in both dollars and time, should be put into building such facilities, and it is important to underscore the maintenance aspect. Such testbeds cannot just be built one time and declared complete; they are ongoing projects that must be sufficiently funded to support their operation, maintenance, and evolution to meet user needs.

Question 2: I am proud of the University of Illinois Champaign-Urbana's leading role in guaranteeing that our Nation's critical infrastructure is resilient and secure. Many of these projects rely on critical funding from the National Science Foundation, U.S. Department of Energy and U.S. Defense Advanced Research Projects Agency.

Can you describe how you collaborate with industry and the Federal Government on these efforts? What priorities should Congress focus on for future investment?

Answer 2:

Collaboration with industry and the Federal Government happens at many levels. We engage with asset owners and industry early in the research lifecycle to discuss problems they are facing that lack immediate solutions. The best way to summarize this is that we look for gaps in the solution space, work with industry broadly to prioritize the areas that require research, and then work with industry and the Federal Government to solve problems and get the solutions into practice. Our approaches include development of open-source technology, licensing to existing companies, and creation of startup companies to commercialize technologies for which there isn't an equivalent elsewhere. In every engagement, it is key to ensure that the stakeholders learn from the nascent science of cyber security and resilience as well as the failures and improvements in other domains. Our role is to tailor that knowledge to the particular domain, develop new scientific advances to address the problem space, work toward developing a solution that is deployable, and work with the government and industry to get it to market and into the hands of the end-users that need it.

In the above, one of the difficult tasks we have been successfully undertaking is to develop the mutual trust needed to have those initial conversations, and then follow through by working toward solutions that solve the problems faced by industry. Technology developed in our research efforts is in active use by asset

U.S. Senate Committee on Energy and Natural Resources
October 11, 2018 Hearing
An Examination of Blackstart, the Process for Returning Energy to the Power Grid after a System-Wide Blackout, and Other System Restoration Plans in the Electric Utility Industry
Questions for the Record Submitted to Timothy M. Yardley

owners around the world because we have transitioned that technology to existing or newly formed companies. Our focus is on accomplishing fundamental research, developing transitionable solutions, and then successfully getting those solutions into the hands of the end users. It all starts from trust, and that takes time for anyone to build.

Question 3: Last year, the Global Information Security Workforce Study found that by 2022 the U.S. will face a workforce shortage of 1.8 million cybersecurity professionals. This will force the industry to increase its efforts to attract, train and retain cybersecurity professionals from an increasingly proportionate small group of qualified personnel. Absent a surge in our Nation's cyber labor force, it is clear why you stated in your testimony that our Nation's cybersecurity workforce is our "weakest link" in protecting our Nation's grid.

In order to sufficiently prepare for the ever increasing threats to our grid, can you explain how a cybersecurity workforce shortage will impact our Nation's ability to initiate a blackstart event and how the workforce shortage is impacting utilities ability to prepare for a large-scale critical infrastructure attack? Similarly, how do we ensure utilities have sufficiently trained and educated personnel to prevent or respond to cyberattacks on the grid?

Answer 3:

I appreciate the underscoring of the cyber labor force shortage, as it is a very important topic. The picture for critical infrastructure is even more grim. The cybersecurity professional shortage will cause a race for the best assets in that space, and the restricted candidate pool will likely be highly courted. Candidates will prioritize opportunities to work for companies that are viewed as exciting or are willing to pay top dollar for the most qualified staff. Where does that leave the nation's critical infrastructure companies? The reality is that the top-tier Silicon Valley companies will likely attract and retain most of the best talent, leaving areas like critical infrastructure in the dust. That outcome doesn't reflect the true relative importance of the two domains, but it's very much the reality we have seen over the past decade.

Correcting the situation will be difficult, but it must be corrected. If we don't have the right talent preparing, defending, and restoring our critical infrastructure, we will be in a grave position. Some of the personnel shortage could be addressed through utilization of third-party contractors that bring in the right staff when needed, but that would not scale in a large-scale attack. Rather, we must staff critical infrastructure with the right talent from the top tiers of the capability pool, and we must systemically address security throughout organizations to make sure that our critical infrastructure is protected and that we are in a strong position to respond if necessary. How we go about accomplishing that may be quite simple. Companies must convey the importance of these positions, create an environment that is exciting and supportive of those who work in it, be open to funding solutions, and compensate people in a way that reflects their true market value.

Question 4: In your testimony, you highlighted the importance of both cybersecurity and cyber resiliency. It is critical to pair these two preventive measures because no system can be perfectly protected. However,

cyber resiliency is considered a lower priority and because of this inequality, the power grid's ability to recover from successful cyberattacks suffers.

Can you explain why cyber resiliency does not get sufficient attention and support? What resources does the grid require to balance the two protective measures?

Answer 4:

The answer is simply that the difficulty of achieving cyber resiliency increases with the complexity of the system in question—and the U.S. electric power grid is one of the world's most complex machines. Resiliency is often addressed only after the base cyber protections are in place, and the engineering of a broader and more resilient solution space may be extremely complex. The grid's mixture of legacy and modern systems adds difficulty in determining a resiliency approach that can scale and can incorporate the complexities of the modern resources while still working within the restrictions of the legacy resources.

The industry as a whole has been making progress on cyber security and perimeter-level protection. Features have been enhanced, new products are on the market, and new technologies and practices have been deployed in the field. What we lack is sufficient understanding of what is technically needed, implementable, and affordable to get us to the point that we have true cyber resiliency in the face of a determined adversary. In addition, the mindset needs to shift from just focusing on more protection and the defense-in-depth approach, to a realization that all such protections will fail and that we must operate through those failures or recover quickly from them. It's something that every cyber security professional recognizes, but more investment needs to be put into building tools, requiring changes in manufacturing designs, and training people on what to do when things do fail and how to recover quickly while minimizing the impact of the attack.

DIESEL TECHNOLOGY FORUM

October 11, 2018

STATEMENT

Before the United States Senate Committee on Energy & Natural Resources

Concerning the Full Committee Hearing to Examine Black Start

In today's highly connected, digital and integrated world, uninterrupted electrical supply is well beyond convenience. It is a necessity. Loss of grid power creates broad economic, public health, safety and security concerns. A report by the Council of Economic Advisors estimates that the average outage costs between $18 billion and $33 billion. Severe weather events, mechanical failures and cybersecurity concerns all pose a growing threat to our electrical generating and distribution network, and our reliable, continuous electrical supply.

In the event of a power station/grid failure, restoration of electrical power to the generating unit is through a black start process, involving a generating unit that can restart its own power without support from the grid in the event of a major system collapse or a system-wide blackout.

Effective, tested plans, systems and procedures to ensure continuous electrical power, as well as plans for contingencies in the event of the loss of generating system capabilities or grid connectivity, are essential roles of government and system operators as well as underlying technology providers.

Diesel-powered generators are an integral part of the black start plan for most system operators for several reasons.

- **Proven Technology:** For many decades, diesel has been the technology of choice for electrical power generation for stand-by, backup and critical load-carrying capacity due to its combination of attributes (below).
- **Superior Response Time**: Diesel generators go from a start condition to full load-carrying capacity in 10 seconds.
- **Superior Load-Carrying Capacity**: Diesel generators are able to handle the full electrical demand load immediately at start-up, while other technologies could take several minutes to full load capacity.
- **Maximum Design Flexibility and System Integration**: Diesel generators can be sized for any application. Diesel engines are typically used in the black start system for gas turbine units up to 35 megawatts, but larger frames need multiple auxiliary generators, which are readily available.
- **Readily Available Fuel Supply, With Safe Storage**: Diesel is the most energy-dense liquid fuel that is readily available, replenish-able and can be safely stored in large quantities.
- **Established Service and Support Networks:** Diesel generators are supported by a broad, established network of service providers with ready access to parts across the United States.

- **Maximum Portability**: Unlike other fuels and technologies, diesel generators with self-contained fuel storage are available in mobile configurations for flexible deployment and utilization even to the most remote locations.

Beyond black start capabilities, mobile and stationary diesel generators along with diesel fuel are a proven and reliable source of both prime and backup power generation – and have been for decades. These units are prided for their reliability, durability, portability and baseload power capabilities.

The importance and confidence in diesel technologies used for emergency backup power is evident here in the nation's capital, where more than 160 diesel generators are deployed by the government of the District of Columbia and provide emergency backup power to schools, hospitals, shelters, courts, police and firehouses, correctional facilities, universities, and utilities in the event of an outage.

The Diesel Technology Forum is a not-for-profit educational organization representing the leaders in diesel engines, including those that manufacture stationary and mobile generators, as well as vehicle and equipment manufacturers, component suppliers, emissions control technology companies and fueling interests. Resources to learn more about diesel technology in power generation and providing black start capabilities include.

- **Caterpillar:** https://www.cat.com/en_AU/by-industry/electric-power-generation/Articles/Testimonials/cogeneration-protects-sensitive-processes-kyocera.html
- **Cummins:** http://www.ryanwilks.com.au/wp-content/uploads/2010/02/Colongra.pdf
- **MTU Onsite Energy:** https://www.mtuonsiteenergy.com/solutions/black-start-diesel-generators/
- **Deere:** https://www.deere.com/en/engines-and-drivetrain/generator-drive-engines/standby-stationary/
- **Volvo Penta:** https://www.volvopenta.com/industrialpowergeneration/en-en/home.html
- **Yanmar:** http://www.yanmar-es.com/
- **Isuzu:** https://www.isuzu-tk.com/isuzupower.htm

To learn more about diesel technology including specific data about the numbers and types of diesel applications on the road and at work in your state, *please visit our website at www.dieselforum.org*

Diesel Technology Forum Staff Contacts:

Allen Schaeffer
Executive Director
Diesel Technology Forum
5291 Corporate Drive, Ste 102
Frederick, MD 21703
(301) 668-7230
aschaeffer@dieselforum.org

Ezra Finkin
Director of Policy and External Affairs
Diesel Technology Forum
5291 Corporate Drive, Ste 102
Frederick, MD 21703
(301) 668-7230
efinkin@dieselforum.org

GRID ASSURANCE™

Written Testimony of Chad A. Heitmeyer
Vice President of Regulatory Affairs, Grid Assurance, LLC
For the U.S. Senate Committee on Energy and Natural Resources

The purpose of the hearing on October 11 was to examine black-start, which is the process for returning energy to the power grid after a system-wide blackout, and other system restoration plans in the electric utility industry.

Introduction

Chairman Murkowski, Ranking Member Cantwell, and Members of the Committee, thank for the opportunity to provide written testimony. My name is Chad Heitmeyer. I am currently the Vice President of Regulatory Affairs for Grid Assurance, LLC ("Grid Assurance"). I am providing written testimony to emphasize the need for enhanced critical system restoration plans for the electric utility industry. With increasing concerns about the possibility of prolonged transmission grid outages due to natural forces (extreme weather) or human attack (physical or cyber), Grid Assurance was formed to answer a need in the electric industry – the need to restore the electric grid more quickly following a high-impact, low-frequency event. Grid Assurance, offers an innovative and cost-effective way to enhance utilities' ability to recover from catastrophic losses of transmission equipment. This no-regrets option deserves careful consideration by transmission owners and regulators, given ever-present risks to the grid.

About Grid Assurance

Grid Assurance will provide subscribing utilities with access to an inventory of spare transmission equipment in order to respond to catastrophic grid emergencies. In particular, Grid Assurance will (1) maintain an optimized inventory of newly manufactured critical long lead-time spare transformers, circuit breakers and related transmission equipment, (2) provide secure domestic warehousing of the inventory of spares in strategic locations, and (3) offer preplanned transportation and logistical support for prompt release and delivery of spare equipment to utility subscribers as needed to respond to emergencies.

Grid Assurance seeks to address a critical national security need – supporting the resiliency of the bulk power system in the event of a catastrophic event such as a natural disaster or an attack

– by making critical replacement equipment for the transmission grid readily available. The availability of an optimized inventory of long-lead-time critical spares, housed in one or more strategically located, secure domestic warehouses, will allow for faster restoration following attacks on the grid, natural disasters, and other events that damage critical transmission equipment. This unprecedented spare equipment service is designed to help shield consumers from the devastating impacts of prolonged transmission outages. Thanks to economies of scale, diversification, improved logistics, and other efficiencies achieved through centralized inventory management and operations, the resilience benefits realized by Grid Assurance subscribers are expected to come at a significantly lower cost than could be achieved by individual utilities acting alone.

For these reasons, owners of 31 transmission utilities nationwide have evaluated, signed the subscription agreement, are pursuing regulatory approvals and plan to enhance the resilience of their own transmission facilities as subscribers with Grid Assurance. On the basis of subscriber commitments, Grid Assurance expects to place initial orders for equipment inventory in early 2019 and to make inventory available to subscribers through its sparing service in late-2019. Grid Assurance will continue to bring on additional subscribers.

Services of Grid Assurance

Grid Assurance will procure and maintain an inventory of new spare large power transformers, circuit breakers, and other critical transmission equipment. It will provide ready access to spares to subscribing utilities following catastrophic events. The inventory will be built based upon the needs of subscribing transmission owners and then grouped into multiple "equipment classes" with common specifications (e.g., voltage, MVA, impedance). Each equipment class will have a target inventory optimized and be managed to meet the collective needs of transmission owners that subscribe to equipment in that class.

Grid Assurance will warehouse its inventory in secure domestic locations away from affected substations. Grid Assurance currently intends to initially maintain two warehouse locations. The warehouses will be located in areas that meet criteria for long haul transportation facilities, security, topology, weather, and environment.

Grid Assurance also will assist with delivery logistics. Grid Assurance will perform ongoing logistics planning and maintain expertise in large asset transportation, including intermodal transportation for inbound and outbound inventory. Grid Assurance will develop and periodically update subscriber information pertaining to the delivery logistics of the long-haul portion of the transportation of inventoried spares from Grid Assurance warehouses to specific destinations within the subscriber's service territory. Grid Assurance will develop advance

logistic plans that include engineering drawings, load securement drawings, railway clearances, load layout including transportation equipment, and specific transportation routes. These advance logistic plans can be developed by Grid Assurance on behalf of subscribers because the physical location of critical assets and the exact specifications (manufacturer, weight, dimensions, etc.) are known. These advance plans will allow efficient and expeditious delivery in times of emergency.

Grid Assurance will also contract with equipment manufacturers to periodically test, service and maintain equipment in inventory and will manage its inventory so that manufacturer warranties are preserved for subscribers. This ensures that the inventoried equipment will be in working condition and can be moved into place expeditiously following a catastrophic event.

Regulatory Approvals

Utilities are hesitant to make major investments without some level of regulatory assurance that their "prudently incurred" costs will be recouped in rates. Grid Assurance has sought and received certain regulatory declarations from FERC that reduce the regulatory barriers faced by FERC-regulated public utilities to begin subscribing to Grid Assurance sparing service[1]. As a result of these declarations, no regulatory approvals are required from FERC for public utilities subject to FERC's jurisdiction, whether affiliated with Grid Assurance or unaffiliated, to subscribe to Grid Assurance sparing service. In these orders, FERC confirmed that Grid Assurance sparing service can play a role in compliance with NERC reliability standards (Reliability Standard CIP-014). FERC also addressed cost recovery issues for prospective subscribers. It found that utility decisions to subscribe to Grid Assurance sparing service and to purchase spare equipment following a qualifying event are prudent. And, FERC found that existing FERC-approved formula rates or single-issue ratemaking procedures can be used to recover Grid Assurance costs.

Grid Assurance is a prudent part of a contingency strategy and will help to ensure that transmission service is restored quickly and cost effectively after a catastrophic event.

[1] *See Grid Assurance LLC*, 152 FERC ¶ 61,116 (2015); *Grid Assurance LLC*, 154 FERC ¶ 61,244, *order granting clarification and denying reh'g*, 156 FERC ¶ 61,027 (2016).

Conclusion

As threats to the grid continue to emerge, utilities must take additional steps to enhance confidence in their ability to recover promptly and restore service to consumers. The Grid Assurance solution builds on options our industry developed. Options like mutual aid which provide utilities with a quick influx of trucks and people. But mutual aid, alone, is not enough – relying on other utilities' equipment that is "where is, as is and if is" is no longer sufficient. Having immediate access to long-lead-time equipment is imperative for rapid and more complete restoration of the grid following high-impact, low-frequency events.

Thank you for holding the October 11 hearing to examine blackstart. Grid Assurance acknowledges the efforts of the electric sector in responding to the recent extreme weather events, but there will be a time when mutual assistance alone is not adequate. Therefore, we need to continue the discussion and push to improve our industry's level of preparedness. I hope my testimony provides the Committee some insight to a new "no-regrets" option for U.S. and Canadian transmission utilities to participate in today and capable of further enhancing grid resilience. Grid Assurance and its participants strongly support a secure and resilient U.S. bulk power grid that has an adequate supply of critical long-lead time equipment to enhance the ability of the Nation's utilities to respond more quickly to major grid disruptions. We share your goal of protecting this nation's critical infrastructure and appreciate your efforts to address this national security issue. Grid Assurance would be glad to meet and speak with the Committee about the service it offers, the important issues related to restoration of service, and how Grid Assurance can be a tool for supporting rapid recovery efforts for all transmission owners nationwide.

Chad A. Heitmeyer
Vice President of Regulatory Affairs,
Grid Assurance, LLC
1 Riverside Plaza
Columbus, OH 43215
614-716-3303
caheitmeyer@gridassurance.com

