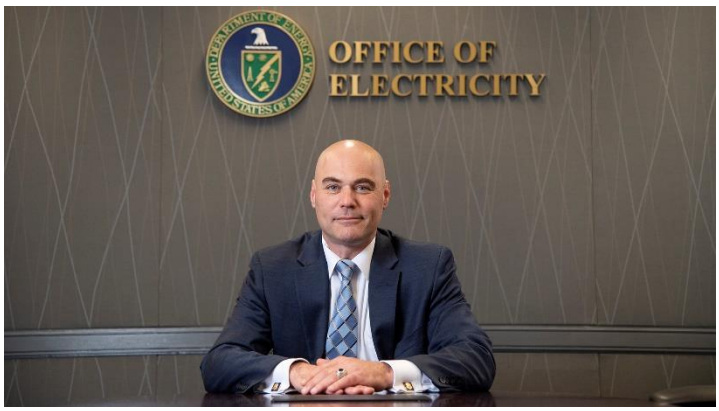
The U.S. Department of Energy's Office of Electricity: A Discussion with Bruce Walker, Assistant Secretary

April 2, 2020

Bruce Walker is the Assistant Secretary for the Office of Electricity at the U.S. Department of Energy (DOE). Confirmed by the U.S. Senate in October 2017, he is responsible for leading national efforts to develop technologies that enhance the security and reliability of energy infrastructure, including work done by DOE's 17 National Laboratories. Under Mr. Walker's leadership, DOE has introduced the North American Energy Resilience Model to assess risks to the electric grid.



Assistant Secretary Bruce Walker
Office of Electricity
U.S. Department of Energy

Mr. Walker also has more than 25 years of electric utility industry experience, including working at National Grid as the Vice President of Asset Strategy and Policy, and for Consolidated Edison of New York, where his last position was Director of Corporate Emergency Management. He played a pivotal role in helping bring New York's power supply back online after the historic 2003 blackout.

The Lexington Institute's Paul Steidler spoke with Assistant Secretary Walker about important electricity matters.

STEIDLER: Thank you for getting together. In January 2019, the Director of National Intelligence raised serious concerns about the cyber threats that the United States is facing from our enemies in both testimony and a report to the U.S. Senate. What do you think of his assessment?

WALKER: The 2019 Worldwide Threat Assessment, which is what you are referring to, clearly states on pages five and six the threats that we have from nation-states, particularly Russia and China. It indicates to the average reader and the industry at large that Russia has a foothold in our electric system, as does China in our pipeline natural gas system.

The intent was to dispel any beliefs as to whether it was true or not true, recognizing that the Office of the Director of National Intelligence pulls together the various agencies within the intelligence community to make those informed decisions. The intent was also to heighten the awareness of the utility industry so that they could make necessary investments and operational changes, while also provide them situational awareness to the threats and how we are dealing with them.

STEIDLER: That sounds quite important.

WALKER: It's a significant challenge. We recognize that cybersecurity or the whole concept of cyber didn't exist when much of the baseload natural gas pipelines' generation transmission systems were built throughout the United States. And really until 2001, people didn't think a domestic attack on U.S. soil was even possible.

So, I think we're facing a different paradigm for which none of the utility bulk infrastructure was designed to take into account. That said, the industry is taking a lot of precautions and moving very quickly to improve their cyber position. Cyber and physical remain number one and two from a risk threat profile from our vantage point.

STEIDLER: How great are the risks in the cyber and physical areas? And what about risks of other manmade or natural events?

WALKER: Well this industry has dealt with, and deals with, risk daily. So, it's not new to the industry to deal with risk. Traditionally, as you noted, we've dealt with things like hurricanes and tornados and torrential wind events -- things of that nature -- as a normal course of business. We've been able to evolve the system to meet the demands or challenges of those risks.

Dealing with cyber and physical risks, especially cyber risks, is completely asymmetrical to the system as compared to a hurricane or a tornado.

Physical risks are not quite as asymmetrical, though the system was not designed to anticipate things like people strapping themselves to a transformer and blowing it up or shooting transformers like we saw at the Metcalf Transmission Substation in California in 2013.

The bulk of the cyber and physical threats are vastly different from natural events because they involve malintent. So, once we start involving nation state actors, we are dealing with vastly different capabilities and a different focus on taking the system down for a variety of different reasons. This is completely different than when we deal with just natural events. But cyber and physical attacks are very, very serious events.

I'm proud to say that industry, DOE, FERC (Federal Energy Regulatory Commission) and NERC (North American Electric Reliability Corporation) are all very focused on these types of attacks. We have millions of pieces of equipment on the system throughout the United States and transitioning them all to being cyber-proof and protecting them from physical attack takes time, effort and a significant amount of investment.

STEIDLER: In July 2019, your office unveiled the North American Energy Resilience Model. What is the mission of that program and what are some of the notable developments?

WALKER: The North American Energy Resilience Model (NAERM) is intended to model all energy infrastructure at the bulk power system level throughout North America.

Over time, there have been some interdependencies that occurred for a variety of reasons. There are many more participants in the bulk power system with the advent of things like wholesale markets, bringing in the regional transmission organizations (RTOs) and many other factors. You have natural gas dependencies that have grown from cheap natural gas. This is great for consumers but challenges the ability of the energy system to have complete situational awareness at any given point.

The purpose of building the Model was to provide the federal government, working with Canada and Mexico, situational awareness to understand the real time happenings of the North American system.

If you identify potential cyber events as well as potential significant events such as those that caused the 2003 Northeast blackout, pre-emptive actions can be taken.

From a planning perspective, the Model will highlight and potentially provide some opportunities for investments that would save expenses like congestion charges. NERC has been very involved in this with some of the RTOs.

The Model will help identify where we should strategically place things like megawatt-scale storage. We'll understand where oscillations, harmonics and other electric phenomenon may be happening on the system. As such, we can use the Model to make decisions at a federal level or a state level that will ensure that our critical infrastructure is available.

STEIDLER: That's great stuff. Grid reliability metrics have always been important, probably no more so than today. But do those metrics need to be examined?

WALKER: Well, the traditional reliability metrics over the last 30 years -- SAIFI (System Average Interruption Frequency Index) and CAIDI (Customer Average Interruption Duration

Index) are fundamentally obsolete in that they have not evolved with what the needs of the system are.

With today's sophisticated computer technology and reliance on data centers, SAIFI and CAIDI are averages. We need to look at different metrics going forward so that we can build the systems to meet the demands of customers. DOE is looking at resilience metrics and rather than go down the metrics path, which we have traditionally done, we are defining classes of customers.

Our most critical infrastructure in the United States, like our defense critical electric infrastructure (DCEI), must have the highest resilience level. So, we are defining the characteristics for that rather than defining the metrics. We will then work with industry to find the other levels of resiliency characteristics needed for important entities like state emergency management centers, hospitals and others.

While they don't rise to the level of a defense critical asset, they obviously are very, very important to public health and safety. As such, they would be high on the priority list. So we will work with industry, NARUC (National Association of Regulatory Utility Commissioners), NASEO (National Association of State Energy Officials) and others to define those attributes and develop solutions. This may require research and development.

STEIDLER: One of the important initiatives of your office has been to help in the development of grid storage technologies. What are some of the notable advances and developments in that regard?

WALKER: We have made some significant movement on large-scale megawatt storage. We have moved away from rare earth minerals, particularly the ones that we don't own and are not ubiquitous.

I said to my team early on that if we want to make it cheap as dirt, make it out of dirt. So, we've made a strong move towards redox equation flow batteries by working throughout our lab complex and universities. We launched the Grid Storage Launchpad (GSL) which is an initiative to build a megawatt-scale storage facility which will provide end-to-end testing for less than 100-kilowatt, bidirectional electric storage.

We initiated that project in fiscal year 2020 and are working with Congress to have it in place in fiscal years 2021-22. We have gone through critical decision-making to place this at the Pacific Northwest National Laboratory (PNNL). We have a design build mechanism in place, and we are working through the final funding. It is a partnership between PNNL, Battelle, and the State of Washington. The idea is to be a public-private partnership and to really accelerate bidirectional electric storage in a very, very big way for utilization throughout our system.

I mentioned earlier the NAERM, the North American Energy Resilience Model. One of the great things it will show is where we utilize storage on our system for things like frequency control, voltage control, black start and whether it's as a source or as a load. So, as we develop this

megawatt scale storage and as we see a high penetration of renewable technology coming onto the system, we're strategically placing storage to help stabilize the system as we move forward.

STEIDLER: And you also work with the Department of Energy's National Laboratories. What are some of the most noteworthy projects that they are undertaking? And how do those laboratories interact with one another?

WALKER: We do work with many of the labs. Most notably we have the Grid Modernization Lab Consortium which is part of the Grid Modernization Initiative.

Through that process, and with the five assistant secretaries in the applied sciences, we co-fund projects that are then competitively bid on by 14 of our National Labs. We go through a very rigorous selection process and we select and award the programs and projects. Just this year alone, we announced $81 million of funding.

In late 2019 we moved forward on the Grid Modernization Lab Consortium (GMLC) process. Each of the departments contributed money. We set guidelines for objectives as to what projects we want and what problems we want solved.

The 14 labs come together, and they lay out the projects they think will solve these problems. We then go through and vet them, adding and subtracting as necessary for each project to meet the needs of the applied sciences. And then we work the projects and they go off and solve the problem.

We anticipate by late spring we'll have our multi-year plan for the Grid Modernization Lab Consortium which will lay out the next three years of what we anticipate doing. And then, subject to appropriations but working with Congress, it's really been a highly productive, highly efficient use of funds. We anticipate that we'll be working through this process for several years.

STEIDLER: And what else is especially important now about the Office of Electricity?

WALKER: So, one of the things we do within the Office of Electricity which is critically important as we work through these cyber risks, the physical risks and through the R&D projects is we also work with four Power Marketing Administrations (PMAs). Three of those PMAs own significant transmission assets in 34 states, covering about two million square miles. Those transmission assets connect to the federal hydro system owned by the Army Corps of Engineers and the Bureau of Reclamation, which is part of the Department of the Interior.

So, the PMAs generate the federal power. We then transport it into the 34 states and feed pretty large customers like our APPA members (American Public Power Association) and NRECA (National Rural Electric Cooperative Association) members as well as a number of investor-owned utilities throughout those 34 states. Those organizations allow us to test a lot of equipment, and do a lot of R&D, for the benefit of their customers.

We fund it through the Office of Electricity. These are real live systems that allow us to really understand what the challenges are within industry. So, our R&D program is informed by our day-to-day operation of those Power Marketing Administrations.

STEIDLER: What are some of the highlights of your recent Congressional testimony?

WALKER: Much of this I covered earlier but there is something very, very significant and really I think a testament to working with our partners within the industry -- electric, oil and natural gas – and with the President's Office of Management and Budget.

We included a separate line item in our fiscal year 2021 budget request called Defense Critical Energy Infrastructure Energy Mission Assurance. This is intended to provide appropriated dollars to do preliminary engineering on defense critical energy infrastructure throughout the United States.

So, as you know, in 2015 the Fixing America's Surface Transportation Act required the Secretary of Energy to define critical defense facilities throughout the United States, and that is my responsibility. Upon doing that, we also defined the defense critical electric infrastructure that is necessary to supply those critical defense facilities.

What we are doing now is utilizing the resources within our Labs, the engineering capabilities in headquarters, and the expertise within our Power Marketing Administrations, and industry writ large, to identify the best investments that we can make to eliminate and mitigate cyber threats and improve our posture for physical threats, as well as protect the system against electromagnetic pulse. All that work falls into that new budget line item this year that enables us to do some of that preliminary engineering.

We will then be able to work with Congress and partners throughout industry to look at making those significant investments. Again, it harkens back to some of the work that Chairman Chatterjee and I were seeking with the FERC/DOE Joint Technical Conference in March 2019.

That work is ongoing and going well. It is focused on identifying the cyber investments and related actions we can do to help our posture from both a cyber and physical threat perspective. There is a lot of work with NERC (North American Electric Reliability Corporation) and FERC (Federal Energy Regulatory Commission) on that, as well as industry through the ESCC (Electricity Subsector Coordinating Council), our international partners and our Power Marketing Administrations.

STEIDLER: Critical defense protection is in your DNA. Please discuss that further.

WALKER: The Office of Electricity's primary function is to meet our requirements and obligation under the FAST Act (Fixing America's Surface Transportation Act). We have responsibility to work with the National Nuclear Security Administration, which is part of the Department of Energy, as well as the Department of Defense, to identify critical defense facilities. We do all the leg work with the electricity industry, understanding the entire supply chain. We work then to define what is required through the FAST Act for defense critical electric

infrastructure. All this is necessary to ensure that these defense critical defense facilities have the capability to complete their missions at any given time.

We work very, very closely with those facilities. We also work very closely with all the energy infrastructure owners that have any part in supplying the energy necessary to help facilities meet their missions.

We also do research and development, including leveraging our weapons labs and other National Labs to identify opportunities for certain technologies and capabilities that benefit energy corridors.

STEIDLER: Anything else?

WALKER: Sensing technologies is another big component of what we're doing.

This is important as we progress down the path of integrating megawatt-scale storage, of utilizing the North American Energy Resilience Model and really looking at providing the ability to see into the system to improve our cyber and physical threat posture. We've been focusing in on and made some significant strides in sensing capability that enables us to see things that have not been seen before on the system due to some of the limitations in our existing infrastructure.

So, things like transformers that have been used in this industry for a hundred years have some ferromagnetic limitations regarding the harmonics and some of the transience they can see.

And as we progress amid increased use of renewables, cyber threats from nation-state actors, potential physical threats from the same, we need to have better situational awareness, better monitoring capability. This applies whether it's electric phenomenon, acoustics or other types of monitoring that enable us to correlate information, working with the intelligence community and other DoE partners like CESER (Office of Cybersecurity, Energy Security and Emergency Response).

We are working with them to take all the data that we have and really understand how it all comes together to provide us the best posture to stave off things like cyber threats, physical threats and simple anomalies that we see on the system and that could potentially impact it like the 2003 blackout.

# # #