Responses to Additional Questions for the Record

The Honorable Fred Upton

You testify that "FERC does not properly assign costs of new or upgraded transmission facilities to the ultimate beneficiaries of those lines." However, isn't equitable cost allocation one of the primary goals of FERC's Order No. 1000? What is your opinion of the Order No. 1000 reforms?

Response of John Hughes:

Unfortunately transmission planning is like rocket science—it is very complex. I believe that FERC was naïve in its approach to transmission planning in Order No. 1000 and did not fully grasp the existing incentive structures (and utility motivations) that complicate efficient planning decisions. Adding a new or upgraded transmission line at some randomly selected location on the grid will always generate benefits somewhere on the system intended or not. That is just the nature of power flows. This does not justify spending an infinite amount of money to get a perfect system. The implementation of Order No. 1000 was flawed because FERC and industry transmission planners have not (1) produced a workably transparent selection process for mapping a specific reliability problem with potential cost-effective solutions; and (2) agreed on a truly equitable cost allocation methodology.

ISOs, RTOs, NERC, and transmission owning utilities are generally very good at identifying reliability problems that need to be addressed and fixed. But there may be multiple ways to solve a specific problem and each approach may have a different set of ancillary benefits and beneficiaries—both short term and long term. FERC allows very lavish compensation for new transmission assets—returns on equity (ROE) are in the 10 to 13% range for relatively low risk investments. This creates a powerful economic incentive to increase the scope of transmission upgrades (by claiming other benefits of the project). Alternative non-transmission solutions are often ignored. One example is utilizing load as a resource (generally called Demand Response). This can defer the need for new transmission that is driven by increased peak demand. ELCON members are increasingly concerned that the transmission costs recovered in their electric bills are getting out of hand with little perceived improvement in grid reliability. They are also concerned that consumer interests are denied adequate opportunity to review the results of the evaluation and selection process.

Cost allocation is equally problematic. The $280 million Artificial Island transmission project (construction of a 230kV transmission line under the Delaware River) is a spectacular example. Depending on the choice of one of three PJM cost allocation methodologies, Delmarva Power & Light's customers would be allocated 93.37%, 6.95% or 10.36% of the $280 million. PSEG's customers would be allocated 0.42%, 42.06% or 18.86%. JCPL's customers would be allocated 0.27%, 13.00% or 12.38%.

Finally I am concerned that the grid operators do not have the necessary human resources and tools for project development, environmental permitting, equipment procurement, and the myriad of other factors associated with transmission development and siting.

Responses to Additional Questions for the Record

The Honorable Robert Latta

1. *In your testimony, you explain how NERC performs a critical role in real-time situational awareness and information sharing to protect critical electric infrastructure:*
   a. *Do you have examples of this real-time situational awareness and how it has helped protect the grid?*
2. *Can you talk more about the Critical Infrastructure Protection Standards that FERC and NERC have worked together on? Specifically, could you talk about the tiered approach to cybersecurity that utilities began to implement in 2016?*

Response of John Hughes:

Historically, NERC directly managed the Interregional Security Network (ISN or NERCnet), an information sharing network used by Reliability Coordinators (RCs) to exchange real-time data with each other. The ISN carries telemetry and system modeling information critical to the monitoring and real-time analysis of the grid's condition. Without this data, it would be much harder for RCs to detect threats emerging from other parts of the electric system. Perhaps more importantly, the data allows them to assess the possibility of a future outage, so steps can be taken before it can manifest itself.

But, as a Compliance Enforcement Authority (CEA), NERC cannot perform a reliability task that is subject to their Reliability Standards. FERC has ruled that this arrangement creates a conflict of interest (*i.e.,* the CEA and the organization responsible for compliance to a standard are one and the same, raising questions of fairness.) Thus, in late 2013, NERC transitioned the ISN to a consortium of Reliability Coordinators.

However, NERC's Operating Committee retains several responsibilities critical to every operator's real-time situational awareness adequacy. This includes Balancing Authorities, Generator Operators, and Transmission Operators; not just RCs. Four obligations come to mind: (1) the analysis of situational awareness outages, (2) the creation of metrics that allows a determination of performance at the individual entity and overall levels, (3) the sharing of best practices and Lessons Learned from incidents, and (4) the assembly of vendors, academics, and industry experts to scope out system and process solutions that address the most imposing issues. ELCON looks to NERC to identify the strategies, practices, training approaches, and platform/ tool improvements that will help reduce the frequency and duration of events that affect real-time situational awareness.

As far as specific examples of important findings identified by NERC – we can think of two recent ones. The first is the investigative work the Operating Committee has sponsored to correlate situational awareness impairments to corrupt or missing input data. We now know that the problem is much larger than previously thought as many instances are masked by the action of backup systems and processes. And, NERC is taking the lead on finding solutions that address

the root problem (*i.e.,* those that detect the sources of data errors and mitigates them without engaging backup capabilities.)

The second example relates to the increasing inability of State Estimator and Real-time Contingency Analyses to converge. The rapid addition of new measuring points, which transmit data at high sample rates, is starting to overload these critical applications. But, once again NERC has taken the lead to find detection mechanisms that will alert front-line Operators to a deterioration in these capabilities. One very promising option caught our attention – a zonal approach where data can be safely accumulated and assessed in small chunks; without a loss in the geographic extent of the wide-area view or its resolution.

Although the Critical Infrastructure Protection (CIP) standards have been mandatory and effective for over nine years, the so-called "Version 5" standards only took effect in 2016. The updates primarily reflect the latest protective strategies available from NIST (Special Publication 800-53) – and security requirements were added for interactive remote access and portable media. The CIP framework now consists of ten very demanding standards addressing physical security, electrical security, account management, configuration control, and information protection; among many other topics.

In the earlier CIP versions, the applicable equipment and systems were determined by a risk assessment developed by each Responsible Entity. Those microprocessor-based servers, work stations, control systems, sensors, and communications systems that could threaten the BES if compromised by a cyber-attack were called "Critical Cyber Assets" and subject to every CIP requirement. Responsible Entities were required to re-assess their asset base every year to assure that newly added Cyber Systems were properly identified and protected.

Although categorization guidelines were provided to the industry, the determination of Critical Cyber Assets varied greatly across the Registered Entity base. FERC determined that this outcome introduced a reliability gap in the BPS, so they directed the creation of bright-line criteria to replace the risk-based assessment strategy. In addition, the Commission called for <u>all</u> Cyber Systems be protected to some extent – even those seemingly of minor consequence. The rationale behind this mandate is that poorly protected Cyber Systems represent a "soft target" to hostile forces, who may use them as a base of operations to launch attacks on interconnected systems of higher importance.

As such, the CIP Version 5 standards include seventeen clear principles that Responsible Entities must apply to identify the most critical BES Cyber Systems and those of medium importance. In general, criticality is determined by the extent of BPS impact that would occur if those assets were compromised by a cyber-attack (*i.e.,* systems that control the greatest amount of power or could destabilize a large geographic area if not available.) All remaining Cyber Systems are deemed to be low-impact.

As one might expect, high-impact BES Cyber Systems are subject to the strictest CIP requirements – driving Registered Entities to focus the lion's share of their protective efforts on them. Medium-impact BES Cyber Systems have nearly as many applicable requirements, but the performance expectations are typically not as demanding. Low-impact BES Cyber Systems are far fewer, but

still require Registered Entities to implement policies for Cyber security awareness, physical security controls, electronic access controls, and incident response.

ELCON sees the tiered approach to cyber security as written in the CIP Version 5 standards as reasonable and effective. We believe that the industry's scarce resources need to be applied to the highest risk systems – and all need to agree which ones those are. In addition, the protective strategies driven by the CIP standards are a challenge to implement, but deliberately crafted to allow Registered Entities to adapt to a rapidly changing cyber landscape. The industry is required to address known and newly emerging threats, but are not locked into using specific technologies and strategies; which can become quickly obsolete in today's environment.

Responses to Additional Questions for the Record

The Honorable Richard Hudson

1. Mr. Hughes, as the Subcommittee has looked at empowering consumers throughout the Powering America hearings, one of the important issues we've seen is fairness and transparency in the electricity rates that consumers pay. Unfortunately, ratepayers are increasingly being forced to finance premium and unnecessary technologies for reasons that have little to do with generating cheap and reliable electricity.

I introduced H.R. 1572, the "Ratepayer Fairness Act," which amends PURPA section 111(d) to require that state public utility commissions consider a fair and transparent process when reviewing requests to subsidize "customer-side technologies" – or technologies that only benefit a few users, but are paid for by everyone else.

In your testimony, you mention that customer interests are consistently underrepresented in the RTO/ISO stakeholder processes.

a. *How would you improve the stakeholder process?*
b. *What more can we do to increase transparency for consumers?*

Response of John Hughes:

1(a). ISO/RTO stakeholder processes are largely driven by the desire of certain stakeholders (mainly utility and merchant suppliers) to keep changing the market rules—changes that might enrich them. Most ISOs and RTOs were established almost two decades ago and the market designs (including pricing mechanisms) have undergone continual change during that time, which keep ISO/RTO stakeholder processes very busy. Since most of the market design changes are intended to force consumers to pay more for their power by creating new revenue streams for suppliers, consumer interests are always in the position of playing defense with only a small fraction of the human resources committed to the stakeholder processes compared to supply interests. The most effective way to improve ISO/RTO stakeholder processes is to limit the need for them. FERC should reach closure on each ISO/RTO market design and not be so amenable to the endless reforms and tweaks coming out of each stakeholder process. Since it is a lot easier for consumer interests to participate in adjudicatory processes at FERC, future reforms should be the subject of formal rulemakings at FERC and not be extensively incubated by ISO/RTO stakeholder processes.

1(b). I am not sure it is possible given that the industry's evolutionary track seems to emphasize greater technological complexity. This, combined with the inevitable legal and economic jargon that pervades a regulated industry, makes for a very daunting task. But I would suggest that utilizing subject matter experts to review these situations is very important and relying more on their assessments than stakeholder group votes can contribute to transparency.