Attachment—Additional Questions for the Record

The Honorable Fred Upton

1. **In your testimony you mention that conventional baseload such as coal and nuclear plants – provide frequency support services as a function of their large spinning generators.**

    a. **What are some of the consequences to deviations in frequency?**

As your question suggests, a reliable bulk power system requires maintaining synchronous generation. The electric grid is designed to operate at a frequency of 60 hertz (Hz). Deviations from 60 Hz can have destructive effects on generators, motors, and equipment of all sizes and types. It is critical to maintain and restore frequency after a disturbance such as the loss of generation. This requires an instantaneous (inertial) response from some resources and a fast response from other resources to slow the rate of fall during the arresting period, a fast increase in power output during the rebound period to stabilize the frequency, and a more prolonged contribution of additional power to compensate for lost resources and bring system frequency back to the normal level.

    b. **Do retirements of conventional baseload units impact frequency?**

Conventional generation units have operating characteristics that can provide essential reliability services necessary for reliable operation of the bulk power system (BPS). As the generation resource mix evolves, the reliability of the electric grid depends upon the operating characteristics of the replacement resources. Specifically, new resources coming online should have the ability to contribute to frequency control of the system.

As conventional generation retires, governor response may decline as the share of variable generation on the system increases. It is common for conventional generators to operate below their maximum rated output, allowing for some governor modulation. This allows the generators to have some flexibility in the upward direction and help support the interconnection response to frequency deviations in a timely manner. Overall, an operating area requires complete capability to manage frequency control for stable system operation.

Simulations of modern wind power plants have demonstrated improved frequency control by implementing fast response to an event at the cost of reducing a portion of its real-power production. Specific levels of frequency response reserves need to be modeled, analyzed, and incorporated in future planning and operating criteria. Specific levels of such support for varying resource mixes will need to be established based on the dynamics of their respective interconnected systems.

c. What policies does NERC have to ensure frequency is consistent?

NERC has a suite of reliability standards that work together to ensure that the system has the ability to maintain a consistent frequency across the grid. NERC Reliability Standard BAL-002-2 requires generation grid operators (known as Balancing Authorities) to recover from a grid event within specified timeframes. The reliable operation of the interconnected power system requires that sufficient resources be available to continuously serve demand and provide contingency reserves that enable the system to respond quickly to lost capacity and energy resulting from forced outages of generation or transmission equipment. In addition, NERC Reliability Standard BAL-003-1 requires those same grid operators to maintain frequency. Frequency deviations are caused when load and generation are not balanced. These grid operators would need excess on-line capacity to make up for any loss of generation to keep the frequency equation in balance. Finally, NERC Reliability Standard EOP-011-1 addresses the effects of operating emergencies by requiring each transmission operator and balancing authority to develop an operating plan (or plans) to mitigate operating emergencies, and that those plans be coordinated between operators.

<u>The Honorable Robert Latta</u>

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 how this real-time situational awareness and has helped protect the grid?

NERC, through both its Electricity Information Sharing and Analysis Center (E-ISAC) and Bulk Power System Awareness (BPSA) departments, maintains real-time situational awareness of conditions and events on the grid that inform NERC's and industry's efforts to protect critical infrastructure and assure reliability.

For example, through the Cybersecurity Risk Information Sharing Program (CRISP), the E-ISAC receives information from either the Department of Energy (DOE) or DOE's Pacific Northwest National Laboratory (PNNL) about anomalies or abnormalities they see in the CRISP data. From there, the E-ISAC is able to work closely with affected entities, DOE, PNNL, and other relevant organizations that can assist with analyzing the data received, identifying potential causes of the anomaly, developing mitigation strategies (if necessary) and communicating to the broader electricity community to monitor their systems for similar activity.

To date in 2017, CRISP has compared more than 18,000 high-value and not publically available threat indicators to data shared by CRISP participants. From those 18,000 indicators, the E-ISAC produced 213 reports that identified potentially suspicious activity. CRISP participants then investigated each report to correlate against internal cyber activity. This private-public partnership

provides a detailed understanding of the intrusion methods, aspirations, and technical proficiency that threat actors employ to evade detection and conduct computer network exploitation and attacks.

CRISP also fosters collaboration among participants on the sharing of indicators of compromise (IOC). To date in 2017, 25% of the CRISP reports are based on information that CRISP participants share. These cases included targeted spear phishing campaigns, redirects to suspicious web pages, and other IOCs. This increased information sharing resulted in enhanced awareness and security for CRISP participants as well as the rest of the electricity industry.

In addition to E-ISAC activities, BPSA maintains real-time situational awareness of the operational status, significant events, and all-hazards threats to the four interconnections across North America. BPSA provides this operational context to E-ISAC as an input to its assessment of security risks to better tailor the E-ISAC's information sharing activities and focus ongoing analyses. Some examples of this interdepartmental collaboration include operational assessments in the hours following the 2013 Metcalf substation shootings that quantified the potential electrical impacts of the attack, "confirm-or-deny" consultations regarding the apparent causes of large customer outages or system disturbances, and triage of multiple simultaneous events to assess the possibility of a coordinated attack on the grid. BPSA also maintains an open line of communication with real-time system operating desks at each reliability coordinator organization to initiate or facilitate rapid information sharing at the "tip of the spear" as needed, as was done during a series of physical attacks on Entergy transmission infrastructure in Arkansas a few years ago.

The E-ISAC has and continues to work closely with cyber security leaders to release actionable information to electric industry companies. The E-ISAC collaborated with the SANS Industrial Control Team to release Defense Use Cases on the 2015 and 2016 cyber security events that impacted Ukraine's electric grid. Additionally, the E-ISAC worked closely with FireEye and DOE to release actionable cyber security information on an advanced persistent threat targeting the energy and nuclear sectors. The E-ISAC continues to collaborate with industry, government, and third-party cyber security organizations to develop and distribute information that electricity companies can use to inform their security postures.

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?**

By expressly stating in the Energy Policy Act of 2005 that reliability standards extend to "cybersecurity protection," Congress had the foresight to anticipate the emerging risk posed by cyber security threats to the bulk power system. NERC's critical infrastructure protection standards (CIP standards) have evolved over time as the nature of threats and vulnerabilities have become better understood. The CIP standards that are currently in effect apply requirements according to impact rating criteria that characterize the level of impact (high, medium, or low impact) of electrical assets, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System. The CIP standards' requirements then

reference those impact categorizations in order to apply commensurately a risk-informed set of cybersecurity requirements. This approach offers increased flexibility in implementing risk mitigation to individual entity operations, enhancing the overall effectiveness of the standards.

The Honorable Gregg Harper

1. **Last year, NERC issued a report which found that "areas with a growing reliance on natural gas-fired generation are increasingly vulnerable to issues related to gas supply unavailability." Can you explain the risks associated with gas supply unavailability?**

NERC recently released a special assessment examining impacts of natural gas supply interruptions, "Potential Bulk Power System Impacts Due to Severe Disruptions on the Natural Gas System." This study as well as our past assessments note that an increasing reliance upon natural gas-fired generation raises important issues for fuel supply security and assurance. The risks are two-fold:

- *The first is **Interruption Risk**. When electric generator customers do not procure "firm" supply and transportation for their fuel, their service is likely to be interrupted when firm customers schedule their full entitlements—particularly in constrained pipeline areas such as New England.*
- *The second is **Curtailment Risk**, which occurs when "firm" service is disrupted through a force majeure event. Curtailments occur when facility outages impact the scheduled flow of natural gas for any reason.*

Understanding the distinction between these two risks is important due to their solutions being very different. For example, electric generation with "firm" fuel service agreements can still be curtailed but can be offset by dual-fuel capability, so long as the back-up fuel inventory is maintained and is not impacted by other issues (e.g., cold weather, for example, can affect the ability of generator to switch-over to a secondary fuel source).

Interruption Risk is generally considered in NERC's annual reliability assessments. Through the assessments, NERC puts a spotlight on generator availability risks that may be impacting their ability to meet peak seasonal demand. However, issues related to generator interruptions are likely to be resolved through integrated resource plans, state or provincial regulatory requirements, and implementation of mitigation strategies—such as dual fuel capability and electricity markets (where they exist). Each of these solutions has a mechanism to consider the reliability needs of the system.

This growing interdependence of the natural gas and electric infrastructure has resulted in new operational and planning reliability challenges. For example, the Aliso Canyon natural gas storage facility leak underscored not only the reliance on natural gas to meet electric demand but also how the disruption of a key natural gas infrastructure component can impact BPS reliability. In addition to natural gas storage, pipelines, compressor stations, and liquefied natural gas (LNG) facilities are

also critical components of the natural gas infrastructure that the electric industry relies on to meet its load-serving obligations. While the natural gas industry has demonstrated a high degree of reliability, the natural gas leak at Aliso Canyon raised awareness of the BPS's dependency on natural gas infrastructure and calls for a closer look at the facilities that support fuel deliveries to electric generation.

The Honorable Bill Flores

1. **As you know, the rapid changes occurring in the generation resource mix and new technologies are altering the operational characteristics of the electricity system and are challenging system planners and operators.**

    a. **How does NERC, through its standards, tackle these challenges?**

NERC has a suite of reliability standards that work together to ensure that the system has the ability to maintain a consistent frequency across the grid. NERC Reliability Standard BAL-002-2 requires generation grid operators to recover from a grid event within specified timeframes. The reliable operation of the interconnected power system requires that sufficient resources is available to continuously serve demand and provide contingency reserves that enable the system to quickly respond to lost capacity and energy resulting from forced outages of generation or transmission equipment. In addition, NERC Reliability Standard BAL-003-1 requires those same grid operators to maintain frequency. Frequency deviations are caused when load and generation are not balanced. These grid operators would need excess on-line capacity to make up for any loss of generation to keep the frequency equation in balance. Finally, NERC Reliability Standard EOP-011-1 addresses the effects of operating emergencies by requiring each transmission operator and balancing authority to develop operating plan(s) to mitigate operating emergencies, and that those plans are coordinated between operators.

In addition, NERC annually reviews the changes in the resource mix with its Long-Term Reliability Assessment to identify potential trends in technology integration. Further, NERC is constantly evaluating events on the system to determine whether emerging technology is creating new reliability risks, and how those risks should be addressed.

The Honorable Jerry McNerney

1. **There's been discussion about the connection between markets and reliability and resiliency. Yet not all states regulators distinguish between reliability and resiliency.**

    a. **Do you believe states should make a distinction between the two?**

System resilience is becoming an enhanced yardstick of reliability. NERC defines reliable operation as "operating the elements of the BPS within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements."[1] NERC is willing to assist states as they consider resilience and reliability matters.

    b. **Does the electric sector use a standard definition of resiliency in both the distribution system and the bulk power system?**

The electric sector has no standard definition of resilience, however the National Infrastructure Advisory Council (NIAC) incorporates widely accepted concepts. The NIAC definition states, "Infrastructure resilience is the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event." NERC would also stress that resilience is already built into many of NERC's efforts, including the importance to learn from events.

    c. **Are there potential benefits to having a more industry-wide accepted term or definition for resiliency?**

There are many different factors to consider. NERC's Board of Trustees recently asked the Reliability Issues Steering Committee to review how NERC's mission currently incorporates resilience of the bulk power system, consider working definitions of resilience, and develop a framework for further discussion at the next NERC board meeting in February.

2. **Is there a standard training for NERC CIP auditors, regardless of the region in which they conduct audits? Has NERC received comments from multi-state IOUs regarding discrepancies in findings, audit results, and interpretations related to CIP compliance?**

NERC provides common training to all auditors, regardless of region, including courses on auditing principles, standards-specific information, and ongoing technical training. NERC provides these in face-to-face settings and through computer-based learning systems. Additionally, NERC facilitates information sharing among CIP auditors through a formalized working group tasked with developing and supporting consistent audit processes. To identify and address any perceived inconsistency, NERC monitors each regional entity's adherence to the regional delegation

[1] *See Glossary of Terms Used in NERC Reliability Standards*.

agreements, the NERC Rules of Procedures, and NERC guidance, as well as policies and procedures. Additionally, NERC administers the ERO Enterprise Program Alignment Process which allows industry to report perceived consistency issues and NERC will track, triage, and resolve consistency issues (this process also allows submitters to remain anonymous).

3. **How can NERC and industry stakeholders improve the number of participants in GridEx?**

NERC's E-ISAC has conducted its biennial Grid Security Exercise (GridEx) series since 2011. Since that time, industry and government stakeholders have demonstrated their commitment to continuing and growing their participation in GridEx. GridEx III in 2015 included 4,400 participants from 365 organizations; this year, GridEx IV had over 6,200 participants from 416 organizations from across industry, the US, state, and local governments, Canada, and Mexico.

The E-ISAC conducted extensive outreach to industry and government at conferences, working group meetings, and through webinars. GridEx received support from major industry trade associations such as the American Public Power Association, the Edison Electric Institute, and the National Rural Electric Cooperative Association, the National Emergency Managers Association, and the National Governors Association. In addition, the E-ISAC worked through cross-sector ISACs to encourage members to participate in GridEx, and we saw direct recruiting of utilities by other utilities. For GridEx IV, cross-sector participants included representatives from the Communications industry, the financial services sector, the downstream natural gas sector, and the water sector.

In addition to this outreach, the E-ISAC continually adds value to the voluntary exercise through an extensive volume of cyber and physical training materials and credit toward cyber and physical certifications for individuals as well as organizational benefits toward compliance requirements such as updating and exercising crisis response plans. The relationships built between electric utilities and local, state, provincial, and federal government departments and agencies is an additional draw toward ever-increasing participation in the extreme cyber and physical attack scenarios.

4. **Is there information on what causes outages or power disruptions – whether it's a squirrel, cyber-attack, fallen tree, etc.?**

Severe weather is the most common cause of bulk electric system (BES) events. Equipment failure in ways unanticipated by design, as well as human error, are other observed factors. NERC's event analysis process assigns appropriate levels of analysis to determine the causes of BES events, promptly assuring tracking of corrective actions to prevent recurrence, and providing lessons learned to the industry. The NERC event analysis process also provides valuable input for training and education, reliability trend analysis efforts, and reliability standards development, all of which support continued reliability improvement. NERC's report – State of Reliability 2017 – provides a detailed and comprehensive analysis of the performance of the BES. This report is produced annually, analyzing the historical risks to the BES with a view toward developing a risk-based approach to solving important Bulk Electric System problems.

5. **How can we properly recognize and value interdependency and cross sector security between oil and gas industries and the electric sector?**

Given the dynamic nature of security threats, cross-sector collaboration is essential. Recognizing interdependencies, the E-ISAC works across many sectors through formal and informal partnerships at both the policy and operational levels.

The E-ISAC participates in daily cross-sector coordination calls with other ISACs to maintain situational awareness of current threats. In addition, E-ISAC staff participate in meetings and coordination with the National Council of ISACs, which provides a forum for sharing cyber and physical threats and mitigation strategies.

In 2017, NERC and the American Gas Association launched a new grid and energy delivery security partnership that takes advantage of the growing interdependency and collaboration of the natural gas and electricity industries. Under the partnership, staff from the Downstream Natural Gas Information Sharing and Analysis Center (DNG-ISAC) joined the E-ISAC in Washington, D.C., to improve coordination on potential security risks related to critical electricity and natural gas pipeline infrastructure. The partnership between the E-ISAC and the DNG-ISAC builds on the long-standing efforts of the gas and electricity industries to address supply interdependencies by developing a robust information exchange on shared security risks.

Finally, NERC is a member of the Electricity Subsector Coordinating Council, which facilitates executive-level coordination between the electricity industry and government officials at the highest levels.

6. **With limited resources, how can we prioritize and identify what to make resilient on the electric grid?**

The production, transmission, and use of electric energy by consumers are dramatically changing. Historically, the system was characterized by centralized dispatch of large synchronous generation and transmission of that power over long-distances to meet customer needs. Currently, the system is moving toward a hybrid model that integrates distributed energy resources and larger amounts of variable renewable resources. The potential impact of these changes must be considered to ensure a reliable and resilient BPS.

Among other initiatives, NERC's Reliability Issues Steering Committee (RISC) identifies and prioritizes many potential risks and makes recommendations to maintain a reliable and resilient BPS. The RISC undertakes a comprehensive review of existing and evolving reliability risks, respective priorities, and evolving character of industry dynamics. It also gathers wide and diverse inputs from industry leaders, associated stakeholder groups, and the regulatory arena. The RISC has convened several Reliability Leadership Summits and a wide-ranging series of focused executive interviews to provide further confidence that key existing and evolving risks to BPS reliability have been identified and captured with no significant issues overlooked. This approach has included resiliency considerations, and has recommended additional industry analysis of common mode failures (e.g. fuel supply failures, extreme weather, transmission corridor outages,

cyber-attacks, cold weather preparation). Industry has responded by participating in cold weather preparation seminars, industry-wide table top exercises on cyber/physical security, and supporting the work plans from the NERC technical committees developed to address evolving and emerging risks to reliability.

7. **What barriers exist for utilities and for the federal government as it relates to utilities sharing resources during emergencies, such as hurricane response?**

The electric power industry maintains a robust and highly effective mutual assistance network which significantly enhances the industry's response and restoration process. Industry and government continue to examine ways to address barriers and further enhance efficient resource sharing. Because the mutual assistance program is exclusive to industry, individual asset operators and their respective trade associations are best positioned to address this important question.

8. **What are the three most common CIP violations, and how often did those occur in 2016?**

Over the past three years, covering 2015, 2016, and 2017 thus far, critical infrastructure protection standards with the highest incidence of noncompliance involved CIP-007 (system security management), CIP-006 (physical security of bulk electric system cyber systems), and CIP-004 (personnel training). NERC's enforcement process assesses the level of risk posed by each instance of noncompliance. Accordingly, it is important to stress that in the vast majority of cases (86%), these instances of noncompliance were assessed to be of minimal risk. 13.4% were of moderate risk; and 0.5% were of serious risk.

9. **To what extent has the increased utilization of distributed energy resources, IoT devices, and other smart grid resources affected the potential sharing of customer data that that is potential threat and vulnerability information as it relates to utility-EISAC information sharing?**

The E-ISAC and NERC do not receive customer data, only information from utilities about potential and confirmed security-related issues detected on their systems. At the customer-utility boundary, distributed energy resources, Internet of Things, and smart grid resources offer new ways for utilities to understand better the issues their customers face, as well as improve efficiency in operations. Aggregated analysis can be voluntarily shared with the E-ISAC but will never contain information about specific customers. In general, these new technologies will certainly help utilities better understand potential and emerging threats, which in turn, help them provide more accurate voluntary reporting to the E-ISAC. The E-ISAC also released an alert in 2016 on the use of IOT devices for high bandwidth denial of service attacks, and in 2017 on supply chain risks.

10. **There is an ever-increasing amount of distributed generation and behind-the-meter technologies and market structures being deployed across the grid. How does additional behind-the-meter activity at the distribution level potentially affect the bulk power system? Is behind-the-meter information and data being shared between utilities, state**

regulators, and federal entities – including FERC, NERC, and DOE? Are there areas for improvement?

As more resources move behind-the-meter to the distribution system and behind the meter, it is increasingly important for planners, operators, and balancing authorities to have visibility into how these resources could affect reliable operation of the BPS. In certain areas, distributed energy resources (DER) are numerous and embedded within a distribution system that has traditionally been viewed as a relatively passive load resource on the BPS. This will no longer be a valid assumption with the integration of more DER on the electric system. There are at least two major events that have occurred on the European power system where the disconnection of DER played a role in system collapse.[2]

In addition, newer DER technologies are capable of providing advanced support services that will be needed as the transition from conventional synchronous resources to nonsynchronous inverter-based resources continues. It is paramount that NERC and the industry understand DER functionality and develop a set of guidelines to assist in modeling and assessments such that owners/operators of the BPS can evaluate and model DER in the electric system. In support of this priority, NERC is developing a set of guidelines to assist in modeling and performing assessments such that owners/operators of the BPS can evaluate and model DER in the electric system. Two guidelines have already been developed and additional guidelines are expected to be completed by mid-year 2018: These can be found at: http://www.nerc.com/comm/Pages/Reliability-and-Security-Guidelines.aspx

Data requirements and information sharing across the transmission-distribution interface should also be further evaluated to allow for adequate assessment of future DER deployments. NERC reviews these issues in a recent report, Distributed Energy Resources: Connection Modeling and Reliability Considerations.

[2] **Italy Blackout 2003:** On the 28th September 2003, a blackout affected more than 56 million people across Italy and areas of Switzerland. The disruption lasted for more than 48 hours as crews struggled to reconnect areas across the Italian peninsula. The reason for the blackout was that during this phase the under-voltage load shedding (UVLS) could not compensate the additional loss of generation, when approximately 7.5 GW of distributed power plants tripped during under-frequency operation. **European Blackout 2006:** In the night of 4 November 2006, at around 22:10, the UCTE interconnected grid was affected by a serious incident originating from the North German transmission grid that led to power supply disruptions for more than 15 million European households and a splitting of the UCTE synchronously interconnected network into three areas. The imbalance between supply and demand as a result of the splitting was further increased in the first moment due to a significant amount of tripped generation connected to the distribution grid. In the over-frequency area (North-East), the lack of sufficient control over generation units contributed to the deterioration of system conditions in this area (long lasting over-frequency with severe overloading on high-voltage transmission lines). Generally, the uncontrolled operation of dispersed generation (mainly wind and combined-heat-and-power) during the disturbance complicated the process of re-establishing normal system conditions.