COMMITTEE ON
ENERGY & COMMERCE
CHAIRMAN FRANK PALLONE, JR.

MEMORANDUM

January 13, 2022

To: Subcommittee on Energy Members and Staff

Fr: Committee on Energy and Commerce Staff

Re: Hearing on "Securing our Energy Infrastructure: Legislation to Enhance Pipeline Reliability"

On **Wednesday, January 19, 2022 at 10:30 a.m. (EST), in the John D. Dingell Room, 2123 of the Rayburn House Office Building, and via Cisco WebEx online video conferencing**, the Subcommittee on Energy will hold a legislative hearing on "Securing our Energy Infrastructure: Legislation to Enhance Pipeline Reliability."

I. BACKGROUND

In the United States, there are over three million miles of pipelines that link natural gas production areas and storage facilities with consumers,[1] and more than 190,000 miles of liquid petroleum pipelines that bring crude oil and refined products to consumers and businesses.[2] These pipelines connect American homes and businesses with the natural gas that accounts for 40 percent of electricity generation[3] and 48 percent of home heating,[4] and the fuel used in automotive and aviation transportation.

Despite our current dependence on these pipelines, there are no federal reliability standards, or any specific entity charged with ensuring delivery of natural gas, crude oil, or other products on energy pipelines. Instead, energy pipelines and natural gas infrastructure are primarily subject to voluntary reliability and cybersecurity measures that have proven inadequate

[1] United States Energy Information Administration, *Natural Gas Explained: Natural Gas Pipelines* (Nov. 5, 2021).

[2] American Petroleum Institute, *Transporting Oil & Natural Gas* (www.api.org/oil-and-natural-gas/wells-to-consumer/transporting-oil-natural-gas/pipeline) (accessed Dec. 1, 2021).

[3] United States Energy Information Administration, *Electricity Explained: Electricity in the United States* (March 18, 2021).

[4] U.S. Department of Commerce, Census Bureau, *Why We Ask Questions About Home Heating Fuel* (www.census.gov/acs/www/about/why-we-ask-each-question/heating/) (accessed December 1, 2021).

to safeguard reliability[5] and security.[6] Two emerging risks highlight the importance of developing a coordinated, federal approach to pipeline oversight in order to protect the health and safety of Americans: natural gas-electric interdependency and the increasing incidence of cybersecurity threats.

II. NATURAL GAS-ELECTRIC INTERDEPENDENCY

According to the North American Electric Reliability Council's (NERC) 2021 Reliability Risk Priorities Report (Risk Priorities Report), critical infrastructure interdependencies, such as the ability to deliver natural gas to electric generating units, is one of the top four risks to the reliable operation of the bulk power system.[7] While the threats associated with this interdependency have long been recognized,[8] the risk to electric reliability has proliferated with the increased use of natural gas in electricity generation.[9] At the same time, natural gas infrastructure itself has become increasingly reliant upon electricity as its main power source.[10] According to the Risk Priorities Report:

> Subsector interdependence continues to increase and has reached an inflection point with the natural gas subsector. Growing reliance on natural gas as an electrical generation fuel source creates the potential for common-mode failures that could have widespread reliability impacts. The dependence of [bulk power system] reliability on natural-gas-fired generation does not align with service priorities within the natural gas delivery system and weatherization requirements for natural gas gathering and delivery systems.[11]

---

[5] Federal Energy Regulatory Commission, North American Reliability Corporation and Regional Entities, *The February 2021 Cold Weather Outages in Texas and the South Central United States*, at 196 (Nov. 16, 2021).

[6] *DHS to issue first cybersecurity regulations for pipelines after Colonial hack*, The Washington Post (May 25, 2021).

[7] North American Reliability Corporation, *Four Interdependent Risks to BPS Reliability Identified in Reliability Risk Priorities Report* (Aug. 13, 2021) and *2021 ERO Reliability Risk Priorities Report*, at 32-33 (Aug. 12, 2021).

[8] NERC Planning Committee, Gas/Electricity Interdependency Task Force, Gas/Electricity Interdependencies and Recommendations (June 15, 2004).

[9] United States Department of Energy, Quadrennial Energy Review Task Force Secretariat and Energy Policy and Systems Analysis Staff, *Electricity Interdependence Memorandum*, at 3 (July 24, 2014); Federal Energy Regulatory Commission and the North American Electric Reliability Corporation, *Report on Outages and Curtailments During the Southwest Cold Weather Event of February 1-5, 2011*, at 189 (Aug. 2011).

[10] Federal Energy Regulatory Commission and the North American Electric Reliability Corporation, *Report on Outages and Curtailments During the Southwest Cold Weather Event of February 1-5, 2011*, at 189; *See* note 7, at 33.

[11] *Id*. and *See* note 7 at 33.

The events of the February 2021 Texas winter storm exemplify the consequences of failing to oversee increased natural gas-electric interdependency. The Federal Energy Regulatory Commission (FERC) and NERC joint investigative report regarding this winter storm (FERC-NERC Joint Report) concluded that "[g]enerating unit outages and natural gas fuel supply and delivery were inextricably linked in the Event," with natural gas fuel supply issues causing more than 27 percent of the generating unit outages.[12] It further states that freezing conditions at natural gas infrastructure and loss of power supply accounted for 86 percent of the decline in natural gas production.[13]

The FERC-NERC Joint Report identifies several recommendations to prevent subsequent wide-scale outages, including that Congress and state legislatures develop plans and measures to better prepare natural gas infrastructure for cold weather and freezing events.[14] It also recommends FERC establish a working group "to improve the reliability of the natural gas infrastructure system necessary to support the Bulk Electric System."[15] This group would explore, among other things, whether Congress should vest one single federal agency with the authority to ensure reliability of interstate pipelines, and how to aggregate and share information between the electric and natural gas systems during emergency events.[16] The report emphasizes the importance of examining natural gas-electric interdependencies and identifies what FERC and NERC have done with their existing authorities to address these issues, concluding that "the time has come for a concerted effort" to solve these issues.[17]

III. CYBERSECURITY

NERC's Risk Priorities Report identifies cybersecurity as one of the main security risks affecting bulk power system reliability, and interdependent infrastructure subsectors, such as natural gas used for electricity generation, are particularly vulnerable.[18] The most recent, high-profile example of cybersecurity exploitation is the Colonial Pipeline cyberattack. On May 7, 2021, Colonial Pipeline Company discovered ransomware on its business systems. To protect the safety of the Colonial Pipeline, the company shut down the Colonial Pipeline's operation.[19] The shutdown of the pipeline, which carries 2.5 million barrels of liquid petroleum products each day from Texas to New Jersey, caused gasoline price spikes and fuel shortages across the East

[12] *See* note 10, at 172.

[13] *Id*., at 175-176.

[14] *Id*., at 193-196.

[15] *Id*., at 195.

[16] *Id.*, at 195-196.

[17] *Id.*, at 196-203.

[18] *See* note 7, at 29.

[19] United States Government Accountability Office, *Colonial Pipeline Cyberattack Highlights Need for Better Federal and Private-Sector Preparedness* (May 18, 2021).

Coast.[20] The Biden Administration tasked the Department of Energy (DOE), the sector-specific agency for cybersecurity in the energy sector,[21] with leading the interagency response to this attack.[22]

The Colonial Pipeline cybersecurity incident prompted the Transportation Security Administration (TSA) to propose its first mandatory cybersecurity standards after relying exclusively on unenforceable guidelines.[23] A Government Accountability Office (GAO) report from 2018 identified several concerns regarding TSA's ability to effectively oversee pipeline system security, including meager staffing levels, lack of a strategic workforce plan to work toward hiring staff with necessary expertise, limited usefulness of its risk assessment methodology, and failure to implement clear, measurable, and effective strategies for monitoring pipeline security reviews.[24] While a more recent GAO report indicates that TSA has addressed some of these issues, it states that TSA still must develop data sources relevant to pipeline threats, vulnerabilities, and consequences of disruption consistent with the Department of Homeland Security's (DHS) risk mitigation priorities, and review and update its 2010 pipeline security protocol plan.[25] One expert recently stated that TSA currently lacks the expertise and resources to oversee a "robust mandatory pipeline security compliance regime."[26]

In response to the Colonial Pipeline cyberattack, FERC Chairman Glick issued a statement, supported by FERC Commissioner Clements, calling for mandatory cybersecurity standards for pipeline infrastructure.[27]

---

[20] *How a major oil pipeline got held for ransom*, Vox (June 8,2021).

[21] United States Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, *Federal Authorities (*www.energy.gov/ceser/activities/energy-security/emergency-preparedness/federal-authorities) (accessed Dec. 1, 2021).

[22] United States Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, *Remarks as Delivered by Secretary Granholm at the White House Daily Press Briefing on the Colonial Pipeline Outage* (May 11, 2021).

[23] *See* note 20.

[24] United States Government Accountability Office, *Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management*, at introduction, 39, and 48 (Dec. 2018) (GAO-19-48).

[25] United States Government Accountability Office, *TSA Is Taking Steps to Address Some Pipeline Security Program Weaknesses*, at 19-20 (July 2021) (GAO-21-105263).

[26] *See* note 6.

[27] Federal Energy Regulatory Commission, *Statement from FERC Chairman Richard Glick: Chairman Glick and Commissioner Clements Call for Examination of Mandatory Pipeline Cyber Standards in Wake of Colonial Pipeline Ransomware Incident* (May 10, 2021).

IV. BULK POWER SYSTEM RELIABILITY

In contrast to pipelines, the transmission of electricity is regulated through a comprehensive framework of mandatory and enforceable reliability standards, including cybersecurity standards. In 2005, Congress added Section 215 to the Federal Power Act (FPA), authorizing FERC to certify an Electric Reliability Organization (ERO) for the purpose of developing mandatory and enforceable reliability standards. In 2006, FERC certified NERC as the ERO.[28]

The U.S. electric utility industry formed NERC in 1968 in the wake of extensive blackouts in 1965. NERC evolved over the years to account for changes in the electricity industry, such as deregulation and increased competition, the shift to increased use of natural gas and renewable energy, and increasing cybersecurity threats.[29]

V. H.R. 6084, THE "ENERGY PRODUCT RELIABILITY ACT"

H.R. 6084, the "Energy Product Reliability Act," was introduced by Rep. Rush (D-IL) on November 30, 2021. The bill directs FERC to certify an Energy Product Reliability Organization (EPRO) to oversee the reliable delivery of energy products on energy pipelines through mandatory and enforceable reliability standards. It is modeled after section 215 of the FPA, which established the statutory framework for FERC's current oversight of the reliability of the electric grid through an ERO.

The bill requires that any standard developed by the EPRO be submitted to FERC for approval before it becomes effective. In addition, the EPRO is required to issue standards that ensure the deliverability of energy products to support electric grid reliability and that protect against cybersecurity and physical security threats. The Energy Product Reliability Act further requires the EPRO to consult with DOE and TSA in developing reliability standards relating to cybersecurity. It also gives FERC authority to establish emergency standards to address continuing or foreseeable emergency conditions under certain circumstances. Finally, the bill maintains much of the same structure included in section 215 of the FPA regarding rules for operation of the EPRO, enforcement mechanisms, and assessment and review of penalties.

VI. WITNESSES

The Honorable Richard Glick
Chairman
Federal Energy Regulatory Commission

The Honorable David M. Turk
Deputy Secretary
U.S. Department of Energy

---

[28] North American Electric Reliability Corporation, *The History of the North American Electric Reliability Corporation*, at 85 (2012).

[29] *Id.*, at vii and 109.