Bernard L. McNamee
[redacted]

March 15, 2023

Kaitlyn Peterson
Legislative Clerk
Committee on Energy and Commerce,
2125 Rayburn House Office Building
Washington, D.C. 20515
Kaitlyn.Peterson@mail.house.gov.

Re: Responses of Bernard L. McNamee to Question for the Record made on March 2, 2023 in relation to appearance on February 7, 2023

Dear Ms. Peterson:

Thank you to Chair Rodgers and Ranking Member Pallone, Chair Duncan and Ranking member DeGette, Chair Johnson and Ranking Member Tonko, the Members of the Committee, and Committee Staff for providing me an opportunity to appear before the Subcommittee on Environment, Manufacturing, and Critical Materials and Subcommittee on Energy, Climate, and Grid Security on Tuesday, February 7, 2023, and to testify at the joint legislative hearing entitled "Unleashing American Energy, Lowering Energy Costs, and Strengthening Supply Chains."

Below are my responses to the QFRs posed by Representatives Griffith and Miller-Meeks.

The Honorable H. Morgan Griffith

1. **I am certainly supportive of energy infrastructure permitting efficiencies such as the interagency pipeline review bill this Committee is considering. It is my understanding that, under the National Environmental Policy Act, the Natural Gas Act, and specifically Title 18 of the Code of Federal Regulations Sec. 380.15, FERC should consider the siting of projects in existing right-of-way. In your experience as a FERC commissioner, does the Commission give due consideration to existing rights-of-way on these applications and in pre-filing discussions?**

McNamee Response Morgan Q1: It has been over two years since I served on the Federal Energy Regulatory Commission ("FERC" or "Commission") and I will not comment on any specific proceeding in which I participated. Furthermore, I cannot testify with personal knowledge as to how FERC reviews have taking place since my term ended. However, I am able to provide a general description of how applications for natural gas pipeline certificates are reviewed by FERC.

There are multiple steps and checks on the Commission when considering an application for a natural gas pipeline. The process for approving a natural gas pipeline under Section 7 of the Natural Gas Act usually begins with the pre-filing process in which an applicant will engage with Commission Staff (primarily the Office of Energy Projects) regarding the proposed pipeline. This provides an opportunity for the applicant and staff to discuss routing issues, including potential use of existing rights-of-way. With the development of either an Environmental Assessment or an Environmental Impact Statement impacts of the propose pipeline on the route are examined. The EA and EIS are initially published as drafts and subject to public comment and are often revised in consideration of those comments. Such comments can also raise issues of rights-of-way. When FERC considers whether to approve a pipeline under section 7 of the NGA, it considers the environmental impacts of the proposed pipeline. Parties can file comments on the proposed pipeline application, including about the rights-of-way. The Commission is supposed to address all of the comments filed in relation to the proposed application for the pipeline, including if rights-of-way issues are raised. The Commission's decisions are ultimately subject to rehearing by the Commission and review by the courts. A simple flow chart of the FERC process is presented on FERC's website.[1]

As a general matter, I believe there are there are likely times where the evidence supports and does not support using the existing rights of way. Those decisions should be driven by the particular facts of the case. But the process should promote the proper consideration of rights-of-way.

2. **How does FERC independently assess and verify multiple projects from different applicants, make use of single rights-of-way? Even if only for a short portion of the project route.**

McNamee Response Morgan Q2: As discussed above, it has been over two years since I served on the Federal Energy Regulatory Commission ("FERC" or "Commission") and I will not comment on any specific proceeding in which I participated. Furthermore, I cannot testify with personal knowledge as to how FERC reviews have taking place since my term ended. However, I surmise that the process described in McNamee Response Morgan Q1 would help ensure that such use of rights of way by multiple projects was utilized as appropriate.

[1] FERC, Natural Gas Certificate Process, https://www ferc.gov/sites/default/files/2020-04/FERCNaturalGasCertificateProcess.pdf (accessed March 13, 2023)

The Honorable Mariannette Mill-Meeks, M.D.

While I do not represent a district on the east coast, I was struck last May by a top U.S. fuel pipeline operator, Colonial Pipeline, shutting its entire network after a cyber attack that involved ransomware. Colonial is the source of nearly half of the U.S. East Coast's fuel supply, and the incident is a prime example of how vulnerable U.S. energy infrastructure is to hackers. I am fully aware of the consequences of a cyberattack t energy infrastructure in my district.[citation omitted]

1. What sort of actions can Congress take to reduce the vulnerability of domestic pipelines and electric infrastructure to cyber-attacks?

McNamee Response Mill-Meeks Q1: The threats from foreign adversaries and non-state actors on American energy infrastructure are real and continue to grow.[2]

Background on current efforts to protect energy infrastructure from cyberattacks.

The federal government has multiple agencies and initiatives working on assisting the private sector protect energy infrastructure. These agencies include, the Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) and the Department of Homeland Security.

As discussed on the Department of Energy's CESER website these initiatives include:

> Industry partners include the Electricity Subsector Coordinating Council (ESCC), the Electricity Information Sharing and Analysis Center (E-ISAC), the Oil and Natural Gas Subsector Coordinating Council, and industry-led research partnerships. Federal partners include DHS via the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Science & Technology, and the National Cybersecurity and Communications Integration Center (NCCIC); NIST Smart Grid Interoperability Panel (SGIP); DARPA; DOD and others. In particular, CESER is a member of the Networking and Information Technology Research and Development (NITRD) program that provides a forum for inter-agency coordination of networking and information technology research activities.[3]

In addition, "[t]he Cybersecurity and Infrastructure Security Agency (CISA), through the National Risk Management Center (NRMC), is working with government and industry

---

[2] U.S. Department of Energy, "Securing America's Energy Infrastructure from Cyber Threats", July 26, 2021 https://www.energy.gov/articles/securing-americas-energy-infrastructure-cyber-threats (accessed March 11, 2023);
[3] U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, Cybersecurity, https://www.energy.gov/ceser/cybersecurity (accessed March 11, 2023)

partners to identify cybersecurity risks and develop strategies to strengthen the security and resilience of the Nation's pipeline infrastructure."[4]

DHS's Transportation Security Administration (TSA) revised and reissued its Security Directive regarding oil and natural gas pipeline cybersecurity in July 2022.[5]

Under the Energy Policy Act of 2005, FERC oversees the reliability of the bulk power system (a/k/a "the electric grid"). Under this authority FERC has approved mandatory cybersecurity reliability standards. These standards are developed with the assistance of the North American Electric Reliability Corporation (NERC). These standards are referred to as Critical Infrastructure Protection (CIP) cyber security reliability standards.[6]

My thoughts and recommendations:

The issue with protecting America's energy infrastructure from cybersecurity threats is not merely one of needing more government regulation or standards on the private sector (though such standards can help). Securing our energy infrastructure requires: 1) ongoing vigilance and investment by the private sector to protect assets; 2) government and the private sector sharing threat information with each other on a continual and timely basis; 3) not sourcing critical components (such as chips, switches, and transformers) from hostile nations, like China, and instead obtain such critical technology from American companies and our allies; and 4) establishing a new national security policy (with the resources and personnel to support it) that will make it clear to adversaries that the U.S. government/military will impose economic sanctions and military retaliation for cyber or physical attacks on American energy infrastructure as the situation merits.

Once again, thank you for allowing me to participate in the Committee's important work on behalf of the American people.

Sincerely,

/s/

Bernard L. McNamee

---

[4] Cybersecurity and Infrastructure Security Agency, Pipeline Cybersecurity, https://www.cisa.gov/sites/default/files/publications/fact_sheet_pci_508.pdf (accessed March 11, 2023)
[5] Transportation Safety Administration, TSA revises and reissues cybersecurity requirements for pipeline owners and operators, July 21, 2022, https://www.tsa.gov/news/press/releases/2022/07/21/tsa-revises-and-reissues-cybersecurity-requirements-pipeline-owners (accessed March 11, 2023)
[6] FERC, Cyber and Grid Security, https://www.ferc.gov/industries-data/electric/industry-activities/cyber-and-grid-security (accessed March 11, 2023)