EDDIE BERNICE JOHNSON, Texas
CHAIRWOMAN

FRANK D. LUCAS, Oklahoma
RANKING MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6375
www.science.house.gov

May 19, 2021

The Honorable Jennifer Granholm
Secretary
United States Department of Energy
1000 Independence Avenue, SW
Washington, D.C. 20585

Dear Secretary Granholm:

As you know, the Colonial Pipeline Company was recently struck by a ransomware attack, which prompted the company to announce on May 7, 2021, that it shut down 5,500 miles of pipeline as a precaution.[1] We write to request a briefing on this incident.

As the Sector Risk Management Agency for the energy sector,[2] the Department of Energy (DOE) plays a vital role in securing critical energy infrastructure from cyberattacks. This responsibility includes using the agency's specialized expertise to assist critical infrastructure owners and operators with mitigating threats, assessing sector risks, and supporting security incident management for the energy sector.[3] DOE's knowledge of our energy sector and the nuanced challenges facing various energy assets uniquely positions it to confront this emerging threat to our national security. Though pipeline cybersecurity implicates multiple federal entities such as the Department of Homeland Security's Transportation Security Administration and Cybersecurity and Infrastructure Security Agency, the Federal Energy Regulatory Commission, and the National Institute of Standards and Technology, these threats demand robust and efficient coordination, both among federal entities and with other stakeholders within the energy sector. While DOE recently announced a "100 day plan" to address cybersecurity risks for the

[1] David E. Sanger et al., *Cyberattack Forces a Shutdown of a Top U.S. Pipeline*, N.Y. TIMES, May 11, 2021, https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html.
[2] Fixing America's Surface Transportation Act § 61003(c)(2), 6 U.S.C. 121 note; William M. Thornberry National Defense Authorization Act for Fiscal Year 2021 § 9002(c)(3) (applying the term "Sector Risk Management Agency").
[3] Homeland Security Act of 2002 § 2215(a)(3).

United States electric system,[4] we seek additional information on how DOE's current and forthcoming cybersecurity activities incorporate energy resources transmitted via pipelines.

The Committee on Science, Space, and Technology has broad authority over "all energy research, development, and demonstration" along with the "commercial application of energy technologies" under House Rule X. The Committee must fulfill its responsibility to ensure our federal cybersecurity and physical security programs and research efforts are focused on combating the most serious threats to our energy supply. We request your assistance to better understand DOE's role in protecting our energy sector from cyberattacks, how DOE includes pipelines in its cybersecurity agenda, and the research and development initiatives that are critical to this work. We ask that your office facilitate a briefing for Committee staff on the concerns described above, including an update on this attack and DOE's response, as well as DOE's current and planned engagement with federal and nonfederal entities to address cybersecurity threats, vulnerabilities, and research challenges.

Thank you for your prompt attention to this matter. For any questions, please contact Janie Thompson of the Committee's Majority staff at (202) 225-6375, or Christen Harsha of the Minority staff at (202) 225-6371.

Sincerely,

Eddie Bernice Johnson
Chairwoman
House Committee on Science, Space, and Technology

Frank D. Lucas
Ranking Member
House Committee on Science, Space, and Technology

[4] U.S. DEP'T OF ENERGY, *Biden Administration Takes Bold Action to Protect Electricity Operations from Increasing Cyber Threats* (Apr. 20, 2021), https://www.energy.gov/articles/biden-administration-takes-bold-action-protect-electricity-operations-increasing-cyber-0 (last visited May 12, 2021).