Deputy Secretary of Energy David Turk Testimony

for the Hearing on "Pipeline Reliability and Draft Legislation"

before the House Committee on Energy and Commerce, Energy Subcommittee

United States House of Representatives

January 19, 2022

Good morning, Chairman Rush, Ranking Member Upton, and distinguished Members of the Subcommittee. I appreciate the opportunity to appear before you today to discuss the Department of Energy's (DOE's) role in ensuring the reliability, security, and resilience of our Nation's energy system, including oil and natural gas pipelines.

The energy sector is uniquely critical—providing power and fuel on which all other U.S. critical infrastructure sectors depend to operate. A disruption in our energy system can have a devastating impact on national security, the U.S. economy, and the livelihoods of millions of Americans. We have experienced the devastating impacts of disruption through multiple events just this year.

As the sector risk management agency and lead agency for energy emergency response, DOE is tasked with leading Federal efforts to secure our Nation's energy infrastructure against all hazards, reducing the risks and impacts of cyber and other disruptive events, and supporting restoration and response. These responsibilities stem from various statutes and executive actions, including the Fixing America's Surface Transportation (FAST) Act; Presidential Policy Directives 21 (Critical Infrastructure Security and Resilience), 41 (United States Cyber Incident Coordination), and 44 (Enhancing Domestic Incident Response); and recent National Defense Authorization Act provisions. We manage these responsibilities through a wide variety of partnerships, informed risk management tools and technologies, and effective incident response.

DOE Partnerships: Collective Preparedness and Response

DOE assesses and analyzes threats to the energy sector, providing regular unclassified briefings to other Federal agencies, States, and industry, in addition to classified threat briefings to cleared industry and State partners. The Department works closely with the three energy sector Information Sharing and Analysis Centers (ISACs)—electricity, downstream natural gas, and oil and natural gas—to disseminate any emerging and potential threats and mitigative measures in a timely manner.

DOE coordinates daily with the two Energy Sector Coordinating Councils—the Electricity Subsector Coordinating Council (ESCC) and the Oil and Natural Gas Subsector Coordinating Council (ONG SCC) include owners and operators and 26 trade associations covering the entire oil and gas supply chain across the U.S. and Canada, and 30 chief executive officers (CEOs) and trade associations representing the electricity sector. Nearly a decade of coordination has resulted in strengthened planning, relationships, and trust that are critical to tackling the evolving threats to our energy sector.

DOE and the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) Co-Chair the Energy Government Coordinating Council (EGCC) to ensure coordination across the interagency on security and resilience issues facing the energy sector. The EGCC includes departments and agencies with energy equities like the Transportation Security Administration (TSA), the Department of Transportation's Pipeline and Hazardous Materials Safety Administration (PHMSA), the Federal Energy Regulatory Commission (FERC), and the U.S. Coast Guard, along with state representatives and international partners. The success of DOE and the energy sector in *collective preparedness and response* is well proven and often serves as a model for other critical infrastructure sectors.

DOE Risk Management Tools and Technologies

DOE and CISA are taking affirmative measures through a set of 100-day sprints directed by the White House to increase the visibility of cyber threats targeting industrial control systems in the electricity and natural gas pipelines sectors. DOE is empowering owners and operators through technology and training to gain a better understanding of the cyber footprint of their information technology (IT) and operational technology (OT) networks. These efforts are being well coordinated with our partners in CISA, TSA, and PHMSA.

In July 2021, DOE released the second version of the Cybersecurity Capability Maturity Model (C2M2) and supporting cybersecurity risk assessment tools. In its first iterations, the C2M2 model was used by hundreds of companies globally to evaluate, prioritize, and improve their cybersecurity capabilities. Nearly 150 cybersecurity practitioners from more than 70 energy sector organizations, including pipeline owners, operators, and trade associations, provided input to the development of the updated version. DOE is also working closely with the oil and natural gas industry and the National Institute of Standards and Technology (NIST) to develop a Liquefied Natural Gas (LNG) Cybersecurity Framework Profile for the energy Marine Transportation System. The Framework Profile may be later modified for application for land-based LNG facilities. Additionally, DOE is working with CISA and NIST on the development of energy sector-specific industrial control systems cybersecurity performance goals. Taken together, the increased visibility, maturity model, and goals will continue to move the sector in the right direction.

DOE also administers a testing program aimed at addressing supply chain risks in critical hardware and software systems used in the energy sector. The program, Cyber Testing for Resilient Industrial Control Systems (CyTRICS™), can help address supply chain threats. The CyTRICS program is a best-in-class program with significant support from industry CEOs, interagency partners, and supports recommendations outlined in the Cyberspace Solarium Commission Report. With electricity, oil, and natural gas companies all relying on similar industrial control systems, DOE is also working with major vendors to improve the security of their equipment that is used to operate critical pipelines, as well as the electric grid, through efforts including the Cyber-Informed Engineering Framework.

In support of States, DOE provides public utility commissioners and energy officials with guidance and risk assessment tools to enhance their energy security planning. These efforts bolster State strategies to mitigate and respond to energy emergencies, as well as build resilience against future events. For

example, DOE has hosted regional petroleum shortage workshops that result in focused plans that outline roles and responsibilities and emergency allocation programs.

The need for long-term energy security planning at the State level is especially pronounced given the complexity of oil and natural gas infrastructure and the interdependencies with the electricity and other critical sectors. Thoughtful planning can ensure strategic investment in new infrastructure, deliver reliability, avoid economic harm, enhance just and equitable emergency response, and reduce environmental impact throughout a State. State efforts will be bolstered by the energy security planning requirement, administered in coordination with the State Energy Program, that was included in the bipartisan *Infrastructure Investment and Jobs Act*.

Response and Restoration

When Federal support is required to restore the energy system, DOE stands up its energy response organization. Incidents like the February 2021 winter storm response across the Central U.S. and the May 2021 Colonial Pipeline incident demonstrated the effectiveness of a whole-of-government response.

The winter storm across the Central U.S.—with impacts felt throughout our Nation—emphasized the need for improved reliability and highlighted the mutual dependencies between natural gas and electric generation. During the event, DOE stood up unity of effort and message coordination across the electric and oil and natural gas industries and, after receiving an official request from the Electric Reliability Council of Texas (ERCOT), utilized our authorities under section 202(c) of the Federal Power Act to enable ERCOT to maximize the use of its generation fleet. DOE experts also contributed to the detailed report recently issued by FERC and the North American Electric Reliability Corporation (NERC) on the causes of and major lessons learned from the incident.

The reliability of the energy sector—and the importance of effective response and restoration—were again highlighted by a ransomware cyber incident that led to the temporary shutdown of the Colonial Pipeline that disrupted fuel availability across the Eastern portion of our country. The Department worked together with CISA, the Federal Bureau of Investigation, TSA, PHMSA, the Environment Protection Agency, and FERC to manage the Colonial incident and its aftermath. While the cyber incident itself did not directly impact operational systems, the concern that the ransomware could have potentially spread to the pipeline's operational networks was enough for Colonial to shut down a critical fuel artery in the United States out of an abundance of caution for safety and the environment. DOE's ability to support Colonial in its response efforts depended on experts from across the Department who understood both the cyber forensics and the operational impact of critical pipelines nationwide. Importantly, the Colonial incident highlights the significance of enhancing the cyber visibility of IT and OT networks in energy sector companies, which is the goal of the 100-Day Industrial Control Systems (ICS) Cybersecurity Plan.

Conclusion

DOE appreciates congressional leadership to improve and enhance the affordability, reliability, security, sustainability, and resilience of our energy infrastructure. We very much look forward to working with

the Chairman, Ranking Member, and all other Members to provide our thoughts, feedback and technical assistance. More generally, I am confident that the entire Federal interagency, including DOE, FERC, FBI, PHMSA, CISA and TSA, stands ready to address this complex and ever-changing threat environment.

With respect to the particular topic of this hearing, DOE will continue to work in close collaboration with Congress, the White House and our interagency partners, our state partners, and the oil and natural gas sector to further strengthen the reliability, security, resilience, and climate and environmental footprint of our Nation's pipelines.

At DOE, we particularly want to make sure we are doing all we can to fully leverage DOE's world-class energy, science, and technology capabilities. We have an incredible team—not only at our headquarters, but across our 17 National Laboratories and our four Power Marketing Administrations—that stand ready do to whatever we can to help. DOE sees our role as an all-hazards preparedness and response organization with the right expertise and partnerships that are so critical to our Nation's national security and energy resilience.

In the coming weeks and months, all of us at DOE look forward to further working with you and your colleagues in Congress on these important topics.

Thank you. I look forward to answering your questions.