BENNIE G. THOMPSON, MISSISSIPPI
CHAIRMAN

JOHN KATKO, NEW YORK
RANKING MEMBER

One Hundred Seventeenth Congress
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

May 11, 2021

Brandon Wales
Acting Director
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
Washington, D.C. 20528

Dear Acting Director Wales,

The recent ransomware attack against Colonial Pipeline Company only further highlights the threat posed to our nation's critical infrastructure by cyber adversaries and the potential cascading effects these attacks can cause to our economic security and way of life.

The committee continues to support the Cybersecurity and Infrastructure Security Agency's (CISA) efforts to ensure owners and operators of critical infrastructure have full visibility into the constantly evolving threat landscape, access to free and voluntary services to better understand vulnerabilities across their IT and OT networks, technical assistance and other services to better fortify their connected systems, and incident response assistance to minimize impact in the event of a cyber incident.

Launched in 2018, the Pipeline Cybersecurity Initiative, housed within the National Risk Management Center (NRMC), has shown promise as a voluntary, public-private partnership between CISA, Transportation Security Administration (TSA), Department of Energy (DOE), and a range of pipeline-dominant critical infrastructure stakeholders. It is the Committee's understanding that the core of this initiative revolves around conducting Validated Architecture and Design Review (VADR) assessments on pipeline assets.

These VADR assessments have proven effective at identifying a wide range of potential vulnerabilities within pipeline systems – some of which have been publicly distilled. Better understanding common security flaws and common misconfiguration issues is in everyone's best interests, and these aggregated insights will help enhance national resilience. For this reason, my CISA appropriations request sent last week proposed an increase of 50% for the infrastructure analysis mission in the NRMC's budget.

Now, in the wake of the Colonial Pipeline ransomware incident, ensuring the success, growth, and effectiveness of the Pipeline Cybersecurity Initiative is more important than ever before. The Committee requests a briefing on the status of the initiative, no later than June 1, 2021. Specifically, the Committee would like clarity on the following:

- How many VADRs have been performed to date as part of the initiative?
- How do CISA, TSA, and DOE work together in the process of identifying potential candidates for conducting VADR assessments?
- How are vulnerabilities identified in these assessments mitigated and what resources does CISA offer to assist in the mitigation process?
- Does CISA plan to expand the VADR assessment offerings to pipeline stakeholders beyond natural gas, to eventually include fuel pipelines like Colonial? If so, what is the timeline for that expansion?

Should you have any questions, please reach out to Austin Agrella, Staff Director for the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation.

Sincerely,

JOHN KATKO
Ranking Member
Committee on Homeland Security