Opening Statement – Ranking Member Kathleen Rice
Subcommittee on Transportation Security

Hearing "Pipelines: Securing the Veins of the American Economy"

April 19, 2016

I understand that it's been several years since this Committee last held a hearing on our nation's pipelines, so I think it's important that we're here today to examine how TSA implements and enforces policies regarding pipeline security, as well as the steps the industry takes on their own initiative.

Last week, we held a roundtable briefing with stakeholders in the oil and natural gas pipeline industry, and I was impressed by the confidence they have in their relationship with TSA. They appreciate that TSA understands there's no one-size-fits-all approach to pipeline security.

I was pleased to hear that TSA and the pipeline industry have that kind of constructive partnership with open and honest communication – because there's no question that pipelines are a potential target. With more than 2.5 million miles of pipelines carrying gas, oil and other hazardous materials across the country, an attack against a pipeline could cause major commercial and environmental damage. So it's important that the policies and procedures we put in place to secure pipelines reflect the magnitude of that threat.

I understand that rather than issuing regulations, TSA has implemented several initiatives like the Corporate Security Review – during which, TSA visits the largest pipeline operators to examine their facilities and security plans. I'm interested to learn more about that process –how often TSA conducts these reviews, and what resources they use to inspect pipeline operators.

I'd also like to know whether or not TSA receives input from DHS's National Protection and Programs Directorate when dealing with pipeline security – both physical and cyber. During our roundtable discussion last week, it was clear that when it comes to eliminating vulnerabilities, stakeholders are focused primarily on cybersecurity. Pipeline operators use supervisory control and data acquisition systems to remotely control and observe pipelines.

Cybersecurity is a top priority right now for many industries and government agencies – so I hope to hear more from our witnesses about what pipeline operators are doing to better protect their cyber infrastructure, and how TSA is supporting those efforts and helping to raise awareness about cyber-vulnerabilities.

I know that TSA holds regular conference calls with stakeholders so they can share information and keep open lines of communication. I'd like to hear from our witnesses about how that process works, and whether TSA is providing the actionable information they need to be prepared to identify and address vulnerabilities.

Thankfully, there have not been any successful attacks against our nation's pipeline systems, but there have been attempts – like in 2007, when three men were arrested for plotting to blow up fuel tanks and pipelines at JFK Airport in New York just outside my district. We must remain cognizant of the fact that terrorists are always looking to exploit vulnerabilities, and our pipelines are a major target – so we have to always stay two steps ahead.