Written Testimony of

Andrew J. Black, President and CEO, Association of Oil Pipe Lines (AOPL)
On Behalf of AOPL and the American Petroleum Institute (API)

House Committee on Homeland Security Subcommittee on Transportation Security
Hearing on "Pipelines: Securing the Veins of the American Economy"

April 19, 2016

Thank you for holding this hearing and for inviting me to testify.

I am Andy Black, President and CEO of the Association of Oil Pipe Lines (AOPL). AOPL represents the owners and operators of pipelines that transport crude oil, refined products like gasoline, diesel fuel and jet fuel, and natural gas liquids like propane and ethane, to American workers and consumers.

I am also testifying today on behalf of the American Petroleum Institute (API). API represents all facets of the oil and natural gas industry, with more than 650 members including large integrated companies, as well as exploration and production, refining, marketing, pipeline, and marine businesses, and service and supply firms.

Pipeline Security and TSA

The oil and natural gas industry is committed to achieving zero incidents throughout our operations. Pipeline operators take considerable steps to ensure the safety and security of our personnel, assets and operations. The security of our pipeline systems is a top priority for pipeline operators. Liquid pipeline operators share TSA's goal of pipeline security, and work hard to secure our facilities and networks. Pipeline operators implement many measures and programs in pursuit of our goal of zero incidents. Operators assess threats to pipelines, including security threats, take steps to address them, and share pipeline security best practices industry-wide.

AOPL and API members appreciate the constructive approach the TSA Pipeline Security Division takes with its pipeline security program. Pipeline operators carefully review TSA's *Pipeline Security Guidelines* and *Pipeline Security Smart Practice Observations* when designing and maintaining security plans. Pipeline operators host TSA for pipeline security inspections and Corporate Security Reviews, which our members tell us are challenging, reasonable, and

pragmatic. Follow-up discussions often result in specific improvements to the operator's security program. We do not ask for any changes in legislation or regulations regarding TSA's programs and activities in pipeline security.

Because of the pipeline industry's designation by the Department of Homeland Security (DHS) as a critical infrastructure subsector, we have many opportunities to participate in government programs focusing on promoting security and identifying threats. We participate in the DHS Oil and Natural Gas Sector Coordinating Council established under Presidential Policy Directive 21 on critical infrastructure security and resilience. These activities provide important opportunities for both classified and unclassified discussions of pipeline security threats. In addition, pipeline operators participate in the DHS Regional Resiliency Assessment Program, and regularly participate in TSA pipeline security stakeholder calls to develop industry-wide awareness of issues seen by TSA and by operators. We also participate in the FBI's Infragard process, a government-industry partnership dedicated to sharing information and intelligence to prevent hostile acts against the U.S.

While participation in these efforts is critical to the development of situational awareness, it should be noted that DHS's risk analysis of all critical infrastructure did not designate any oil or natural gas infrastructure into its highest tier of risk. This is due to our industry's diverse geography, redundant systems and the resilience of the sector when responding to events.

Cybersecurity and API Standard 1164

Pipeline operators follow API Standard 1164, *Pipeline SCADA Security*, which helps pipeline operators defend their systems from cyber attacks. The standard requires operators to maintain systems for controlling pipeline operations separate and apart from business systems with internet access. It was developed with a broad group of stakeholders from the public and private sectors, and helps operators protect systems in a rapidly changing and increasingly complex cyber environment.

The broader oil and gas industry, including pipeline owners and operators, have also created several information sharing forums, including the Oil and Natural Gas Information Sharing and Analysis Center (ONG ISAC), to share threat indicators, alerts and information to identify emerging cyber threats. Pipeline operators also participate in the NIST Cybersecurity Framework Roadmap process. These efforts, combined with the intelligence and information operators receive from government sources, help operators better understand their risk and prevent incidents.

Other Industry Pipeline Security Programs

API has also developed several other standards and programs to promote a culture of security, both physical and cyber. API RP 780, *Security Risk Assessment*, defines the recommended approach for assessing security risk widely applicable to the types of facilities operated by the industry and the security issues the industry faces. API RP 781, *Facility Security Plan Methodology for the Oil and Natural Gas Industries*, will build on RP 780 and provides the process to factor risk assessment into the physical and cyber security measures used to secure

operations. This recommended practice should be published later this year. In addition, API has published *Utilizing Intelligence to Secure People*, a guidance document describing some of the resources that are available to the industry to help attain situational awareness in different operating environments.

API created the *Oil and Natural Gas Industry Preparedness Handbook* with support from members and associations throughout the industry, to illustrate how local responses can be aided by established relationships with governments and communities, local, State and regional associations, and how corporate and federal capabilities can facilitate efficient response and recovery at the local level. The Handbook provides a common sense approach for oil and gas owners and operators, local and State industry associations, and public sector partners to build the necessary capabilities to effectively manage the information flow that so often becomes congested during disruptive events.

Oil spill response plans

I want to bring to the subcommittee's attention a pending pipeline policy issue with significant security implications. Pipeline operators prepare and submit to U.S. DOT PHMSA, our safety regulator, oil spill response plans. These response plans detail facilities and plans for first responder and operator response to pipeline emergencies. They contain sensitive security information, such as worst-case spill scenarios, first responder operational information, pipeline control system locations and information, and descriptions of high-consequence areas. As members of this subcommittee can appreciate, this information would provide a blueprint for a terrorist attack on pipeline infrastructure.

In 2012, Congress authorized PHMSA specifically to redact this sensitive security information when making oil spill response plans public in response to Freedom of Information Act requests. However, a provision in the recent pipeline safety program reauthorization bill, S. 2276, passed by the Senate earlier this year, could allow the public to gain access to pipeline security information terrorists could use to plan an attack.

The specific Senate provision, adopted in Committee as an amendment by Senator Markey, would require PHMSA to provide to Congress, upon request, unredacted copies of oil pipeline response plans. AOPL and API support Congress exercising its oversight role over PHMSA and the oil spill response program, and do not object to Congressional Committee leaders receiving these plans. Unfortunately, however, S. 2276 does not provide clear or specific protections against public disclosure of security-sensitive oil spill response plan information obtained by Congress.

PHMSA legal guidance deems the information at issue here, "if disclosed, would be of significant operational utility to a person seeking to harm the pipeline infrastructure of the U.S." Like PHMSA, we believe this information must be protected from public disclosure because of these security risks. We are ready to discuss this with you and with members of this Committee, the Transportation and Infrastructure Committee, and the Energy and Commerce Committee, as pipeline safety reauthorization legislation moves through the House and conference in coming months.

New Threats and Actions Against Pipelines

Finally, there is a growing pipeline security issue operators are watching closely. Opponents to pipeline projects in Canada are breaking into pipeline facilities, tampering with valves, and locking themselves to equipment as part of their protests. There were four incidents[1] between November and January on one pipeline and a fifth incident[2] on another in January. These actions could harm a pipeline operator's ability to respond to an incident and could even unintentionally result in a pipeline release impacting the public or environment.

I understand information from unredacted oil spill response plans has helped some Canadian protestors in choosing where and how to obstruct a pipeline's activities. Information circulated for, or by, pipeline opponents can easily reach terrorist organizations who might intentionally use this information to harm the public. I encourage Congress to keep these new threats in mind when reviewing unredacted response plans and determining how the important information within them should be withheld from public disclosure.

I thank the subcommittee for considering these issues, and would be happy to respond to any questions.

[1] "Pipeline industry concerned about tampering and vandalism", *CBC News*, March 9, 2016, http://www.cbc.ca/news/business/cepa-chris-bloomer-pipelines-tampering-enbridge-vandalism-target-1.3480857.

[2] "Pipeline sabotage: Someone tampered with valve on Enbridge fuel pipeline near Cambridge", *Hamilton Spectator*, January 5, 2016, http://www.thespec.com/news-story/6219719-pipeline-sabotage-someone-tampered-with-valve-on-enbridge-fuel-pipeline-near-cambridge/.