September 28, 2009

Ginger LeMay
Office of Information Technology, TSA-11
Transportation Security Administration
601 South 12th Street
Arlington, VA 20598-6011

VIA FIRST CLASS AND ELECTRONIC MAIL (ginger.lemay@dhs.gov)

Re: *Intent to Request Approval from OMB of One New Public Collection of Information: Pipeline Operator Security Information*

Dear Ms. LeMay:

Pursuant to the 60-day Notice issued in the referenced docket by the Transportation Security Administration ("TSA") on July 28, 2009, and published in the July 29, 2009, issue of the *Federal Register*, 74 Fed. Reg. 37723, (the "Notice"), the Interstate Natural Gas Association of America ("INGAA") submits the following comments.

The Notice solicits public comment on an Information Collection Request ("ICR") that will be contained within the forthcoming Pipeline Security Guidelines (the "Guidelines"). To quote TSA, the Guidelines "will include recommendations for the voluntary submission of pipeline operator security manager contact information to TSA's Pipeline Security Division and the reporting of security incident data to the Transportation Security Operation Center (TSOC)."

INGAA is a non-profit trade association that represents the interstate natural gas transmission pipeline industry. INGAA's members operate over two thirds of the nation's natural gas transmission pipeline mileage. Their interest in the proposed ICR is self-evident.

INGAA does not oppose providing the proposed security manager contact information to TSA's Pipeline Security Division. As detailed below, INGAA has four concerns with the ICR's proposal for reporting security incident data.

1. The potential civil liability associated with these reports must be addressed.

Four of the ten proposed categories of reportable incidents, and parts of at least two others, call for the pipeline to report "suspicious" activity. Yet, with all these references to suspicious activity, the ICR does not expressly address the potential civil liability that arises when such activity is reported but later found to pose no threat to homeland security. Should someone identified in one of these reports fall subject to inappropriate, unwarranted or adverse government examination or surveillance, one can reasonably imagine that person will attempt to seek redress, and the likely defendant will be the pipeline operator, which will not have the benefit of sovereign immunity. To cite Paperwork Reduction Act criterion 3, until the civil liability issue is addressed pipeline operators will have serious reservations about reporting incidents with the "quality, utility and clarity" proposed in the ICR.

2. If the database of reported incidents is going to be used for vulnerability and threat analyses it must be internally consistent, and for the database to be internally consistent the categories of reportable activities must be defined objectively, not by subjective assessments of suspiciousness.

Contrary to Paperwork Reduction Act criterion 2, the ICR proposes to collect information far beyond what is necessary for the proper performance of its functions. INGAA agrees that five of the ten proposed categories of reportable incidents are reasonably objective and describe events that can reasonably be considered significant (or at least potentially significant) threats to homeland security:

- Explosions or fires of a suspicious nature affecting pipeline systems, facilities, or assets
- Actual or suspected attacks on pipeline systems, facilities, or assets
- Bomb threats or weapons of mass destruction (WMD) threats to pipeline systems, facilities, or assets
- Theft or loss of Sensitive Security Information (SSI) (detailed pipeline maps, security plans, etc.)
- Actual or suspected cyber attacks that could impact pipeline Supervisory Control and Data Acquisition (SCADA) or enterprise associated IT systems

Of the five remaining categories, four concern one or another form of "suspicious" activity. Apart from the civil liability issue identified above, defining categories by a subjective standard (in this case, suspiciousness) invites differences in interpretation and inconsistencies within the data being collected. Put simply, pipeline operators can reasonably disagree about what constitutes suspicious activity and whether a specific activity should be reported. If the reported information is going to be used for vulnerability and threat analyses (see *Federal Register* page 37724) it should be as internally consistent as possible. Reporting "suspicious" activity does not meet this standard, and these four categories should be removed.

3. The proposed reporting of thefts of company vehicles, uniforms and credentials runs counter to sound pipeline management policies and threatens to engulf the TSOC in a stream of reports that have no bearing on homeland security.

The tenth proposed category of reportable incidents is thefts of pipeline company vehicles, uniforms, or employee credentials. Experience shows that very few thefts of company vehicles give rise to suspicions of terrorist activity or even a remote threat to homeland security. Pipeline operators report such thefts to local law enforcement, and in the rare case where homeland security issues surface the reporting burden should rest on local law enforcement, not the pipeline that was the victim of the crime.

An even stronger case can be made against reporting "thefts" of company uniforms and employee credentials. Many pipeline policies governing misplaced uniforms and credentials do not distinguish between items that are lost and those that are stolen. There are sound, practical reasons for this approach. It is often impossible to verify whether something that is claimed to be lost was lost, or something that is claimed to be stolen was stolen. Sometimes an employee may claim something was stolen rather than admit losing it, and a lost item can become stolen if it is later found and improperly used by someone else. Although INGAA has not canvassed its members on this issue, it is reasonable to assume pipelines deal with hundreds if not thousands of lost credentials each year, and the vast majority of these incidents pose absolutely no threat to homeland security. INGAA members handle "lost or stolen" cases internally, with at most a handful requiring the involvement of local law enforcement. Flooding the TSOC with a stream of lost credential incident reports will not only fail to advance TSA's mission, it will hinder that mission by wasting agency resources on reports with no meaningful tie to homeland security.

4. In an effort to minimize the reporting burden, TSA should coordinate with other federal and state authorities to establish a single point of contact and a single security incident reporting form.

INGAA recommends TSA coordinate with other federal, state and local authorities to develop a single point of contact and single form for incident reporting. INGAA members are subject to both comprehensive economic regulation by the Federal Energy Regulatory Commission and comprehensive safety regulation by the U.S. Department of Transportation's Pipeline and Hazardous Materials Safety Administration. These and other federal agencies, as well as hundreds of state and local officials, all want to be apprised when a security-related incident occurs on an interstate natural gas pipeline. As a result, INGAA members currently spend inordinate time reporting the same incident over and over to official

after official. One of the objectives of the Paperwork Reduction Act is to "minimize the burden of the collection of information on those who are to respond." To achieve that end TSA and its sister agencies — federal, state and local — should work together to develop a unified report so a pipeline can report an incident one time through a single point of contact.

One final note is in order. The ICR calls for information to be provided voluntarily. By design, the comments presented above would be equally appropriate if the proposed reporting were mandatory. Civil liability exposure, overbroad and unnecessary data categories and inefficient information collection are serious issues, and it would be inappropriate to claim they do not have to be addressed because reporting is voluntary.

INGAA appreciates the opportunity to comment in this docket and offers its continued assistance in the development of a measured, objective and efficient program for reporting incidents that impair or meaningfully threaten homeland security.

Respectfully submitted,

Dan Regan
Regulatory Attorney
Terry D. Boss
Senior Vice President for
Environment, Safety and Operations
Interstate Natural Gas Association of America
10 G Street, N.W., Suite 700
Washington, DC 20002
(202) 216-5900