BRACEWELL

INSIGHTS

As Cyberthreats Continue, PHMSA and TSA MOU Stresses Information Sharing and Coordination

March 20, 2020

*By: **Catherine D. Little**, **Annie Cook** and **Mandi Moroz***

The Pipeline and Hazardous Materials Safety Administration (PHMSA) and the Transportation Security Administration (TSA) recently finalized an ***Annex*** to a longstanding Memorandum of Understanding (MOU) regarding pipeline safety and security. This Annex comes just weeks after a publicized natural gas pipeline cybersecurity ***intrusion*** and responds to several recommendations from the Government Accountability Office (GAO) discussed in our earlier ***alert*** to update the prior Annex which had not been reviewed or revised since its inception over 14 years ago. The updated Annex emphasizes information-sharing and coordination between the agencies and signals that the agencies are moving forward on satisfying outstanding GAO recommendations. While this is a step in the right direction, questions remain whether TSA is the appropriate agency to oversee pipeline security and whether existing voluntary standards should be mandatory.

Since September 11, 2001, the U.S. oil and gas pipeline network has been a target of both physical security and cybersecurity threats and intrusions. In particular, oil and gas pipelines are a potential terrorist target due to the possibility of both the disruption of critical product supplies across the country and impacts to the public and the environment. The Department of Homeland Security issues cyber vulnerability alerts almost on a daily basis to the energy industry, but many intrusions are not widely publicized because operators typically report them to and address them with the FBI, and they are treated as classified information.

PHMSA, with the Department of Transportation, is responsible for regulating pipeline *operational safety*, while the Department of Homeland Security's TSA is responsible for pipeline *physical safety and cybersecurity*. Both PHMSA and TSA have come under increased scrutiny from Congress and others to update outdated agreements and provide for mandatory security measures. TSA in particular was criticized for being largely understaffed, with a team of only five or so employees in this area who lack cybersecurity experience, and for failing to send a representative to Congressional Pipeline Safety Act reauthorization hearings. Existing TSA security standards remain voluntary and were last updated in 2018 in TSA's 2018 ***Pipeline Security Guidelines***. Other relevant documents, however, ***have not been updated*** to better reflect more recent cybersecurity threats and means to address those threats.

Revised provisions of the Annex provide for information sharing through an "interagency protocol" with respect to incidents and security threats and expressly note that the agencies will coordinate prior to conducting inspections of cross border facilities that are operated from control rooms in Canada. The agreement also includes new language regarding coordination with DHS’s Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Energy and in particular with regard to response and recovery efforts following natural and man-made disasters. Strategic planning will also include consensus concerning measures to minimize the consequences of man-made and natural disasters involving pipelines. Much of the remainder of the updated Annex, however, is not new.

Although PHMSA has not historically held itself out as an expert in security issues, close cooperation and resource sharing between PHMSA and TSA may enhance TSA’s ability to more effectively address the issues the industry has been facing. PHMSA and TSA have committed to reviewing the MOU at least once every five years, to ensure their strategies and efforts remain up to date and revise it when needed. That said, given the ongoing pressures on the industry from security and cybersecurity threats, and the government for managing those threats, the possibility of mandatory requirements remains.