Billing Code: 4910-60-W

DEPARTMENT OF TRANSPORTATION

Pipeline and Hazardous Materials Safety Administration

[Docket No. PHMSA-2016-0137)

Pipeline Safety: Safeguarding and Securing Pipelines from Unauthorized Access

AGENCY: Pipeline and Hazardous Materials Safety Administration (PHMSA); DOT.

ACTION: Notice; Issuance of Advisory Bulletin.

SUMMARY: PHMSA is issuing this Advisory Bulletin in coordination with the Department of Homeland Security's (DHS), Transportation Security Administration (TSA), to remind all pipeline owners and operators of the importance of safeguarding and securing their pipeline facilities and monitoring their Supervisory Control and Data Acquisition (SCADA) systems for abnormal operations and/or indications of unauthorized access or interference with safe pipeline operations. Additionally, this Advisory Bulletin is to remind the public of the dangers associated with tampering with pipeline system facilities.

This Advisory Bulletin follows recent incidents in the United States that highlight threats to oil and gas infrastructure. On October 11, 2016, several unauthorized persons accessed and interfered with pipeline operations in four states, creating the potential for serious infrastructure damage and significant economic and environmental harm, as well as endangering public safety. While the incidents did not result in any damage or injuries, the potential impacts emphasize the need for increased awareness and vigilance.

FOR FURTHER INFORMATION CONTACT: Operators of pipelines subject to regulation by DOT, PHMSA, should contact Nathan A. Schoenkin by phone at 202-366-4774 or by email at Nathan.Schoenkin@dot.gov. Information about PHMSA may be found at http://phmsa.dot.gov. Pipeline operators with questions on TSA's Pipeline Security Guidelines should contact Steven Froehlich by phone at 571-227-1240 or by email at Steven.Froehlich@tsa.dhs.gov.

SUPPLEMENTARY INFORMATION:

I. Background

Incident Details

On Tuesday October 11, 2016, individuals contacted four pipeline operators informing them they would shut down the pipelines used to transport crude oil from Canada to the United States. The operators (Enbridge, Kinder Morgan, Spectra Energy, and TransCanada) took steps to prevent damage to the pipelines and contacted local and federal law enforcement. The individuals cut the chains and padlocks at valve sites near Leonard, Minnesota; Burlington, Washington; Eagle Butte, Montana; and Wahalla, North Dakota. The individuals then closed valves on Enbridge's Lines 4 and 67, Spectra Energy's Express Pipeline, and TransCanada's Keystone Pipeline. The Kinder Morgan Trans Mountain's Puget Sound Pipeline was not operating at the time. Several individuals were arrested by local law enforcement.

Had the pipeline operators not shut down their lines in response to the threats, a pipeline rupture could have occurred. A pipeline rupture due to tampering with valves can have significant consequences such as death, injury, and economic and environmental harm.

Pipeline Safety and Security

PHMSA and TSA have a mutual interest in ensuring coordinated, consistent, and effective activities that improve interagency cooperation on transportation security and safety matters. PHMSA focuses on the safety of the Nation's pipelines and administers the pipeline safety regulatory program (49 CFR Part 190-199). TSA focuses on the security of the Nation's pipelines and has authored Pipeline Security Guidelines for operators available online at https://www.tsa.gov/sites/default/files/tsapipelinesecurityguidelines-2011.pdf.

II. Advisory Bulletin (ADB-2016-06)

To: Owners and Operators of Hazardous Liquid, Carbon Dioxide and Gas Pipelines

Subject: Safeguarding and Securing Pipelines from Unauthorized Access

Advisory: PHMSA is issuing this Advisory Bulletin in coordination with TSA to remind all pipeline owners and operators of the importance of safeguarding and securing their pipeline facilities and monitoring their SCADA systems for abnormal operations and/or indications of unauthorized access or interference with safe pipeline operations. Additionally, this Advisory Bulletin is to remind the public of the dangers associated with tampering with pipeline system facilities.

If You See Something, Say Something™

Tampering with pipeline facilities can have deleterious effects on the safety of the Nation's pipeline system. Tampering or acts of sabotage can also lead to the loss of life, injury, and significant harm to the economy and environment. At 49 CFR 190.291, any person that

willingly and knowingly injures or destroys, or attempts to injure or destroy a pipeline facility is subject to a fine in Title 18 of the United States Code and imprisonment for a term not to exceed 20 years for each offense. Individuals are reminded that "If you See Something, Say Something"™ applies to the safety and security of our national pipeline infrastructure. Individuals that see something suspicious should reach out to their local law enforcement. Informed, alert communities play a vital role in keeping our Nation's energy infrastructure safe. Emphasizing that "Homeland Security Starts with Hometown Security," DHS encourages businesses to "Connect, Plan for, Train, and Report". Tools and resources to help businesses plan, prepare, and protect themselves from suspicious activities or attacks are located online at https://www.dhs.gov/hometown-security.

Relationships with Local Law Enforcement

PHMSA reminds pipeline operators that a strong relationship with local law enforcement is extremely beneficial for safe pipeline operations. Two-way communications between operators and law enforcement can help to stop threats before they occur. Relationships should be cultivated well in advance of an incident to facilitate mutually dependable communication during an incident.

Increased Security Patrols

Pipeline operators should consider increasing the frequency of security patrols along their right of ways. Operators may want to consider the use of new technologies to aid in pipeline security patrols, such as unmanned aerial systems if authorized in the areas of operation. Frequent patrols may help inform pipeline companies of individuals who regularly congregate near a pipeline, or

of potentially unsafe conditions at a valve or pump station. Information regarding suspicious individuals should be promptly forwarded to federal, state, and local law enforcement.

Protection of Facilities

PHMSA's Office of Pipeline Safety requires pipeline operators to provide protection for valves on hazardous liquid pipelines at 49 CFR 195.420(c). Additionally, at 49 CFR 195.436, hazardous liquid pipeline operators are required to provide protection for each pumping station, breakout tank area, and other exposed facility from vandalism and unauthorized entry. Furthermore, at 49 CFR 192.179(b)(1), natural and other gas pipeline operators must ensure that the valve and operating device to open or close the valve must be protected from tampering and damage. PHMSA recommends that pipeline operators review their valve and facility protection measures and consider taking additional steps to secure them.

Operators should evaluate what type of locks and security fences are being used at valve stations and if they are capable of preventing unauthorized personnel from gaining access to pipeline valve facilities. Pipeline operators may choose to make mechanical operation of valves more difficult without proper equipment.

The use of deterrent text and signage at pipeline facilities may be beneficial to decrease acts of sabotage against a pipeline facility. The text should include the potential consequences if a valve is closed improperly and a rupture was to occur. Additionally the deterrent text should include reference to the PHMSA regulation found at 49 CFR 190.291 discussing the criminal penalties

for tampering with pipeline facilities. Remote facilities should consider equipping the facilities

with motion sensing cameras and/or motion detectors to alert control centers of tampering.

SCADA System Monitoring

Due to the criticality of SCADA systems in the safe operations of a pipeline, operators should

have strong protocols in place to ensure the systems will not be tampered with. SCADA systems

can be tampered with or disabled by a physical or cyber vector. PHMSA is aware of prior

intrusion attempts on pipeline infrastructure. An operator should harden physical and software

borders around SCADA systems to limit the risk to the safe operation of pipelines. The

following methods can be used to harden the software and physical borders around the SCADA

system: [1] Segregating the control system network from the corporate network; [2] Limiting

remote connection ports to the control system, and if necessary requiring token-based

authentication to gain access; [3] Adding physical protection around remote sites with SCADA

network access; [4] Enhancing user access control on SCADA system networks and devices and

limiting access to critical system to individuals with a safety/business need; and [5] Employing

application whitelisting and strict policies on peripheral devices (to include removable media,

printers, scanners, etc.) connected to the SCADA network.

Furthermore, DHS's Industrial Control System Cyber Emergency Response Team (ICS-CERT)

developed a guidance document titled: "Recommended Practice: Improving Industrial Control

System Cybersecurity with Defense-in-Depth Strategies." The document provides guidance for

developing mitigation strategies for specific cyber threats and direction on how to create a

Defense-in-Depth security program for control system environments, and is available online at

https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-

CERT_Defense_in_Depth_2016_S508C.pdf.

Incident and Accident Reporting

Operators are reminded that incidents and accidents must be promptly reported to the appropriate

federal, state, and local agency. Requirements for immediate notification of certain incident and

accident reporting requirements are found at 49 CFR 191.5 and 195.52. Furthermore, since

tampering with a pipeline can lead to a release, PHMSA recommends that operators should

contact the National Response Center by telephone to 800-424-8802 (in Washington, DC, 202-

267-2675) following any physical security event that may interfere with the safe operation of a

pipeline. Please note only "*unclassified*" incident details should be reported by phone to the

National Response Center.

TSA recommends in its Pipeline Security Guidelines that pipeline operators notify the

Transportation Security Operations Center via phone at 866-615-5150 or email at

TSOC.ST@dhs.gov as soon as possible to report security concerns or suspicious activity.

Furthermore it is recommended that pipeline operators notify DHS's ICS-CERT if the operator

has an Industrial Control System concern with a cyber security nexus. Operators can report to

ICS-CERT by emailing ics-cert@hq.dhs.gov or by calling 877-776-7585.

PHMSA has coordinated with several components within DHS and the Department of Energy on

this Advisory Bulletin.

Issued in Washington, DC on December 5, 2016, under authority delegated in 49 CFR 1.97.

Alan K. Mayberry,
Acting Associate Administrator for Pipeline Safety
[FR Doc. 2016-29500 Filed: 12/8/2016 8:45 am; Publication Date: 12/9/2016]