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 12–8–16; 8:45 am]

BILLING CODE 4910–60–P

DEPARTMENT OF VETERANS AFFAIRS

MyVA Federal Advisory Committee; Notice of Meeting

The Department of Veterans Affairs (VA) gives notice under the Federal Advisory Committee Act, 5 U.S.C. App. 2., that the MyVA Advisory Committee (MVAC) will meet January 10–11, 2017, at the Department of Veterans Affairs, Georgetown University Lohrfink Auditorium—Ground Floor, Georgetown McDonough School of Business, Rafik B. Hariri Building, 37th and O Street NW., Washington, DC 20057. The meeting is open to the public.

The purpose of the Committee is to advise the Secretary, through the Executive Director, MyVA Task Force Office, regarding the MyVA initiative and VA's ability to rebuild trust with Veterans and other stakeholders, improve service delivery with a focus on Veteran outcomes, and set the course for longer-term excellence and reform of VA.

On January 10, from 8:00 a.m. to 6:00 p.m., the Committee will convene an open session to discuss the progress on and the integration of the work in the five key MyVA work streams—Veteran Experience (explaining the efforts conducted to improve the Veteran's experience), Employees Experience, Support Services Excellence (such as information technology, human resources, and finance), Performance Improvement (projects undertaken to

date and those upcoming), and VA Strategic Partnerships.

On January 11, from 8:00 a.m. to 1:00 p.m., the Committee will meet to discuss and recommend areas for improvement on VA's work to date, plans for the future, and integration of the MyVA efforts. This session is open to the public. No time will be allocated at this meeting for receiving oral presentations from the public. However, the public may submit written statements for the Committee's review to Debra Walker, Designated Federal Officer, MyVA Program Management Office, Department of Veterans Affairs, 1800 G Street NW., Room 880–40, Washington, DC 20420, or email at *Debra.Walker3@va.gov*. Any member of the public wishing to attend the meeting or seeking additional information should contact Ms. Walker.

Dated: December 6, 2016.

Jelessa M. Burney,

Federal Advisory Committee Management Officer.

[FR Doc. 2016–29546 Filed 12–8–16; 8:45 am]

BILLING CODE 8320–01–P