TR 2017-05 – GM – Reporting Security Concerns

PRIMARY: 191, 192.614, 192.613, 192.179
SECONDARY: 192, 192.705, 192.721
PURPOSE: Review existing GM, and revise as appropriate, in light of ADB-2016-06
ORIGIN/RATIONALE: ADB-2016-06 {Federal Register Volume 81, Number 237 (December 9, 2016)}
RESPONSIBLE GROUP: O&M/OQ Task Group

Note: Revisions are shown in yellow highlight and red font.

Section 191.5 {Addendum 4, last paragraph is now (i)}

(j)* Operators are advised by the Transportation Security Administration (TSA) that if an event might have involved a breach of security of the pipeline facility, at the earliest practicable moment, the event should be reported to the Transportation Security Operations Center at 866-615-~~6~~ 5150 or TSOC@dhs.gov.

(k)* Operators are advised by the following government agencies that if an event might have involved a breach of cyber-security of the pipeline control system (e.g., SCADA), at the earliest practicable moment, the event should be reported to:
(1) National Cybersecurity and Communications Integration Center (NCCIC) at 888-282-0870.
(2) Department of Homeland Security, ICS-CERT at 877-776-7585 or ics-cert@hq.dhs.gov.

**Note:* See OPS Advisory Bulletin ADB-2016-06 (81 FR 89183, Dec. 9, 2016) and TSA Pipeline Security Guidelines (March 2018); reference Guide Material Appendix G-192-1, Section 2.

Section 192.179

1 VALVE SPACING ON OFFSHORE-ONSHORE PIPELINES
2 BLOWDOWN RECOMMENDATIONS
3 PROTECTIONS FROM TAMPERING AND DAMAGE
The operator should consider minimizing the potential risks to the system from unauthorized operation of valves. The operator should consider deterrents where practicable such as the following.
(a) Underground vaults.
(b) Removal of operating wheels.
(c) Chain and locking devices.
(d) Remote controlled valves.
(e) Protected SCADA design for remote controlled valves.
(f) Warning signs stating the consequences or penalties of tampering with the facility. [Suggested in OPS Advisory Bulletin ADB-2016-06 (81 FR 89183, Dec. 9, 2016; reference Guide Material Appendix G-192-1, Section 2).]

Section 192.613 *{June 2023 Note: Updated to Addendum 2 version}*

1 GENERAL
Continuing surveillance should be conducted to identify any pipeline facilities experiencing abnormal or unusual operating and maintenance conditions. This may be accomplished by the following.
(a) Periodic visual inspection of pipeline facilities to identify items such as the following.
(1) Changes in population densities.
...
(6) Potential for, or evidence of:

(i) Excavation activity.
Note: If evidence of an excavation is found near a transmission pipeline covered segment, the location must be examined in accordance with §192.935(b)(1)(iv).
(ii) (ii) Tampering, vandalism, ~~or~~ damage, or suspicious activities possibly leading to acts of sabotage. See guide material under §191.5 regarding reporting of such occurrences.
Note: As appropriate, an operator should report such instances to local law enforcement.
(iii) Earth movement. See Guide Material Appendix G-192-13.
(iv) Flooding. See 6 below.
(v) Mining activity. See Guide Material Appendix G-192-13.
...

(b) Periodic review and analysis of records, such as the following.
(1) Patrols.
...
(7) Facility failure investigations.
(8) Reported vandalism, sabotage or suspicious activities. Tools and resources to help operators plan, prepare, and protect themselves from suspicious activities or attacks are located online at www.cisa.gov/connect-plan-train-report.

Anomalies discovered should be evaluated, and those determined to present potential safety concerns should be scheduled for remediation and communicated to appropriate integrity management personnel.

Section 192.615 *{June 2023 Note: Updated to Addendum 2 version}*

1 WRITTEN EMERGENCY PROCEDURES (§192.615(a))
(a) ...
...
(e) To ensure the safety of the general public, an operator's written procedures should provide for the following as applicable.

1.1 Receiving, identifying, and classifying emergencies.
(a) ...
(b) Instructions to operator personnel should ensure that the information received is evaluated to determine the priority for action. Some situations call for operator personnel to be dispatched promptly for an on-the-scene investigation. Those personnel should respond in an urgent manner giving a potential emergency top priority until the severity of the situation has been determined. Some situations require that priority be given to other actions, such as notification to gas control, other operator personnel, or local emergency response personnel. See 3.3 below.

Examples of emergency situations that require immediate response include the following.
(1) Gas ignition or explosion.
(2) A hissing noise is present or there is any indication of a broken or open-ended pipe.
(3) Report of a pulled service or damaged facility.
(4) Gas odor throughout the premise or building.
(5) Other identified (i.e., operator designated) emergency~~ies~~.
(6) Report of tampering, vandalism, suspicious activity, or unauthorized access. See guide material (j) and (k) under §191.5.
(c) ...

Section 192.631 *{June 2023 Note: Updated to Addendum 2 version}*

1 GENERAL

2 CONTROLLER

3 COMPONENTS OF CONTROL ROOM MANAGEMENT PROCEDURES

3.1 General.

3.2 Controller roles and responsibilities.

Section 192.631(b) requires operators to define the role and responsibilities of the controller during normal, abnormal, and emergency operating conditions.

(a) Normal operating conditions.

...

(b) Abnormal operating conditions.

...

(c) Emergency operating conditions.

(1) Types of emergency operating conditions might include the following.

(i) Overpressurization.

...

(viii) Report of gas in a building and emergency evacuation.

(ix) Report of unauthorized system hacking (cyberattack), physical tampering, or other physical acts of sabotage.

(2) Procedures should contain the following.

...

3.3 Communications.

Communication issues may also be addressed in management of change (MOC) and training in 6 and 7 below.

(a) Communication protocols.

Consideration should be given to the timeliness, type, and amount of information to be passed on to both internal and external entities, and designation of the person responsible for the communication. Internal entities may include other controllers, both on shift and between shifts, and other operator personnel outside of the control room environment such as field technicians, supervisors, and management. External entities may include suppliers, customers, local emergency personnel, electric providers operating within the gas system territory, the National Response Center (NRC), or regulatory agencies. In the case of incidents related to attempted or confirmed breach of security or cyber security, the Department of Homeland Security recommends operators make notifications to its agencies as advised in guide material (j) and (k) under §191.5. Notification criteria can be found in the TSA Pipeline Security Guidelines (March 2018; reference Guide Material Appendix G-192-1, Section 2).

(b) ...

...

3.4 Manual pipeline operation.

...

4 SUPERVISORY CONTROL AND DATA ACQUISITION SYSTEMS

4.1 General. ...

4.2 Controller interface. ...

4.3 Alarm management. ...

4.4 Point-to-point verification. ...

4.5 SCADA system design and monitoring to protect from unauthorized access.

(a) Operators should consider the following methods for securing authorized access by hardening physical and software borders around SCADA systems to limit the risk to the safe operation of pipelines.

(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 systems to individuals with safety or business needs.
(5) Employing application whitelisting (the practice of explicitly allowing some identified entities access to a particular privilege, service, mobility, or recognition – the reverse of blacklisting) and strict policies on peripheral devices (e.g., removable media, printers, scanners) connected to the SCADA network.
(6) Monitoring unauthorized usage.

(b) See references in 10 below.

5 OPERATING EXPERIENCE

6 MANAGEMENT OF CHANGE (§192.631(f))

7 TRAINING (§192.631(h))

8 SHIFT WORK AND FATIGUE (§192.631(d))

9 COMPLIANCE AND DEVIATION

10 REFERENCES

(a) API RP 1165, "Recommended Practice for Pipeline SCADA Displays" (see §192.7 for IBR).
(b) API RP 1168, "Pipeline Control Room Management."
(c) OPS Advisory Bulletin ADB-2016-06, "Pipeline Safety: Safeguarding and Securing Pipelines From Unauthorized Access" (81 FR 89183, Dec. 9, 2016; reference Guide Material Appendix G-192-1, Section 2).
(d) Department of Homeland Security guidance document, "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies." September 2016. Found online at: http://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf
(e) TSA Pipeline Security Guidelines, March 2018.

Section 192.705 *{June 2023 Note: Updated to Addendum 2 version}*

1 GENERAL

Transmission lines and Type A gathering lines should be patrolled, as necessary, to observe factors affecting safe operation and to enable correction of potentially hazardous conditions. In addition to visual evidence of leakage, patrol considerations should include observation and reporting of potential hazards and conditions such as the following.

(a) Excavation, grading, demolition, or other construction activity ...
...
(i) Suspicious persons, activities, or devices in the vicinity of pipe facilities. See guide material under §191.5 regarding reporting of such occurrences to federal authorities. As appropriate, an operator should report such instances to local law enforcement.

2 SCHEDULING

...

3 METHOD

(a) Where practical, the patrol map or other documents (e.g., aerial photographs or videos) used by the person making the patrol should identify areas near the transmission line that might require special attention. ...
(b) ...
(c) ...

4 REPORTS

Patrol reports should indicate hazardous conditions or suspicious activities observed, corrective action taken or recommended, and the nature and location of any deficiencies. These reports should also include information about population density near the right-of-way, including indications such as those listed under 1(h) above.

5 FOLLOW-UP

...

Section 192.721

1 GENERAL

Distribution mains should be patrolled, as necessary, to observe factors affecting safe operation and to enable correction of potentially hazardous conditions. In addition to visual evidence of leakage, patrol considerations should include observation and reporting of potential hazards such as the following.

(a) Excavation, grading, demolition or other construction activity ...

...

(g) Suspicious persons or activities in the vicinity of pipe facilities. See guide material under §191.5 regarding reporting of such occurrences. As appropriate, an operator should report such instances to local law enforcement.

2 SCHEDULING

...

3 SPECIAL LOCATIONS

...

4 REPORTS

Patrol reports should indicate hazardous conditions or suspicious activities observed, corrective action taken or recommended, and the nature and location of any deficiencies.

GMA G-192-1

2 GOVERNMENTAL DOCUMENTS

DHS	Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. Industrial Control Systems Cyber Emergency Response Team (September 2016)	§192.631
OPS ADB-2016-06	Advisory Bulletin – Safeguarding and Securing Pipelines From Unauthorized Access (81 FR 89183, Dec. 9, 2016)	§191.5 §192.179 §192.631
Transportation Security Administration	Pipeline Security Guidelines (March 2018) (https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf)	§191.5 §192.631

4 PUBLISHING ORGANIZATIONS

The specifications, codes, standards, and other documents listed in Sections 1 and 2 are published by the following organizations:

DHS Mail Operations Program Manager
MGMT/CRSO/Mailstop 0075
Department of Homeland Security
245 Murray Lane SW
Washington, DC 20528-0075

6 SUMMARY OF PRIMARY WEBSITES

Department of Homeland Security (DHS)'s National Cybersecurity and Communications Integration Center (NCCIC) and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)	http://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf	§192.631
Department of Homeland Security	www.cisa.gov/connect-plan-train-report	§192.613
Transportation Security Administration	https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf	§191.5 §192.631