2019 – November 13 – Editorial Section

Approved proposed additions and revisions of GM under §§191.5, 192.179, 192.613, 192.631, 192.705, 192.721 and GMA G-192-1. Ready for 2nd LB

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))

LB Processing Note: The proposed changes from LB1-2019 are shown in yellow highlight.

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

(i)* Operators are advised to report security concerns or suspicious activities 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 via phone at 866-615-6150 or email at TSOC@dhs.gov. (See OPS Advisory Bulletin ADB-2016-06; 81 FR 89183, Dec. 9, 2016; reference Guide Material Appendix G-192-1, Section 2.)

(k)* Operators are advised to report possible cybersecurity related events to Department of Homeland Security, ICS-CERT via phone at 877-776-7585 or email at ics-cert@hq.dhs.gov. (See OPS Advisory Bulletin ADB-2016-06; 81 FR 89183, Dec. 9, 2016; reference Guide Material Appendix G-192-1, Section 2.) 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) Motor Remote controlled operated valves.
   (e) Protected SCADA design for motor remote controlled operated valves.
   (f) Warning signs stating the consequences of tampering with the facility.

Section 192.613

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) Damage, tampering, vandalism, 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) Flooding. See 6 below.
   ...

(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 companies plan, prepare, and protect themselves from suspicious activities or attacks are located online at www.dhs.gov/hometown-security.

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 192.631

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.
       ...
       (ix) Report of unauthorized system hacking (cyberattack), physical tampering, or other physical acts of sabotage.
   (2) Procedures should contain the following.
3.3 Communications.
3.4 Manual pipeline operation.
4 SUPERVISORY CONTROL AND DATA ACQUISITION SYSTEMS

4.1 General.
SCADA systems provide controllers with important tools to perform their roles and responsibilities. These tools include instrumentation for monitoring pipeline operating conditions and for operating pipeline equipment. SCADA systems may generate an alarm when an event has occurred or an unusual situation is developing.

The following are the primary components of a SCADA system, with definitions or examples of each.

(a) Field devices.
   (1) Pressure transmitters.
   ...
   (8) Mechanical devices that control compressor engines.
   [moved to 4.5 below] Unauthorized usage monitoring. See 4.5 below.
   Note: Devices that lack communication capability with the control room, such as pressure recorders, gauges, or other field devices that only monitor the pipeline, are not considered part of SCADA.

(b) ...

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."
GENERAL
Transmission 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. "If you see something, say something." 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.

SCHEDULING

METHOD
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 may require special attention. ...

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.

FOLLOW-UP
...
...  
(k) Facilities or support structures that require maintenance, until repaired.  
(l) Facilities identified to be threatened by possible sabotage activity.
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

<table>
<thead>
<tr>
<th>Organization</th>
<th>Description</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHS</td>
<td>The Department of Homeland Security (DHS)'s National Cybersecurity and Communications Integration Center (NCCIC) and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)</td>
<td>§191.5 §192.631</td>
</tr>
<tr>
<td>DHS</td>
<td>Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. Industrial Control Systems Cyber Emergency Response Team (September 2016)</td>
<td>§191.5 §192.631</td>
</tr>
<tr>
<td>OPS ADB-2016-06</td>
<td>Advisory Bulletin – Safeguarding and Securing Pipelines From Unauthorized Access (81 FR 89183, Dec. 9, 2016)</td>
<td>§191.5 §192.631</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Organization</th>
<th>Website</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>--------------------------------</td>
<td>-----------------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>