

PIPELINE SECURITY INFORMATION CIRCULAR

Information of Concern to Pipeline Security Personnel

Security Guidance for Natural Gas, and Hazardous Liquid Pipelines and Liquefied Natural Gas Facilities

Subject: PIPELINE SECURITY GUIDANCE

Issued: September 5, 2002

Summary:

Pipelines represent an important part of the nation's critical infrastructure. Therefore, it is incumbent upon pipeline operators to take appropriate steps to protect critical pipeline facilities. The Research and Special Programs Administration's Office of Pipeline Safety (RSPA/OPS) developed the attached guidance document in cooperation with energy and pipeline trade associations and state pipeline safety programs. This circular and the attached document define critical pipeline facilities, identify appropriate countermeasures for protecting them, and explain how RSPA/OPS plans to verify that operators have taken appropriate action to implement satisfactory security procedures and plans.

These guidelines represent the next step on a continuum of efforts by industry and the federal government to improve the security of the nation's pipelines. The Transportation Security Administration (TSA) is responsible for ensuring the security of the transportation infrastructure and for fostering equivalent levels of protection across all modes of transportation. Because pipelines are an integral part of the nation's energy and transportation infrastructures, RSPA/OPS, the Department of Energy, and TSA are working together to achieve these goals. Pipeline operators rely on RSPA/OPS as their primary source of information for matters related to pipeline safety, including security issues, based on close working relationships forged over many years of daily interaction. While these guidelines may be revised as additional information becomes available, changes will be made only after appropriate consultation with industry. TSA will work with RSPA/OPS to avoid inconsistencies in guidance or unnecessary changes.

An operator's security procedures may be included with a plan for operations, maintenance, and emergency response or in a separate document. OPS does not expect an operator to create redundant plans. We do suggest a cross reference to existing plans. RSPA/OPS and our State pipeline safety partners will not require operators to submit copies of their corporate security plans.

Instead, RSPA/OPS and states will review the plans on site at the operator's offices, and conduct spot checks of selected critical facilities in the field to verify that the operator is implementing its plan as written. RSPA/OPS understands that corporate security plans will likely be limited in their distribution and that field personnel may not be aware of all the details of their employer's security plan. However, when spot-checking facilities that the operator has identified as critical, RSPA/OPS intends to verify the extent to which the operator has implemented the protective measures and security training described in their security plan.

The purpose of this information circular is to encourage operators to identify their critical facilities and to begin to implement appropriate measures for such facilities. RSPA/OPS does not imply that operators must implement every measure identified for each of the various threat levels. Because pipeline facilities may be attractive terrorist targets, operators need to make a good faith effort to implement security measures to protect the safety of the public and their critical facilities, and to ensure reliability of the nation's energy supply both for national defense and to sustain the economy. For facilities that do not meet the threshold for being designated critical, operators may still want to implement some security measures.

Recommendations:

In the current threat environment, all natural gas and hazardous liquid pipeline and liquefied natural gas facility operators should continue and strengthen their security efforts. The following measures or their equivalents are basic:

1. Identify any of its facilities that could be defined as "critical facilities." If an operator considers none of its facilities to be critical, document the basis for the conclusion. The operator should maintain a list of facilities that are identified as critical in a secure place at corporate headquarters. This list should be available to RSPA/OPS and State representatives for on-site verification. RSPA/OPS does not intend to require operators to distribute this list outside the corporation.
2. Develop a corporate security plan that is consistent with the security guidance published by the trade association for the operator's segment of the pipeline industry.
3. Begin to implement their corporate security plan as soon as possible.
4. Review their corporate security plan on an annual basis and revise it as necessary to reflect changing conditions.

Submission of Operator's Statement:

RSPA/OPS requests that within six months of the date of this circular, each operator should submit a written statement to confirm that the operator has:

- reviewed this information circular and the accompanying Pipeline Security Contingency Planning Guidance;

- reviewed the consensus security guidance appropriate to its portion of the pipeline industry;
- identified its critical facilities;
- developed a corporate security plan; and
- begun implementing its corporate security plan as necessary to protect the physical and cyber security of its critical facilities.

For operators under the authority of RSPA/OPS, the statement should be submitted to the Associate Administrator for RSPA/OPS. For intrastate operators, the statement should be submitted to the State pipeline safety regulatory agency. Operators' written statements are needed to confirm that operators are making progress and fully understand what is expected of them, and to enable RSPA/OPS to measure the effectiveness of the current non-regulatory approach to pipeline security.

The statement may be sent to:
 Associate Administrator for Pipeline Safety
 Room 7128
 Research and Special Programs Administration
 U.S. Department of Transportation
 400 Seventh Street, S.W.
 Washington, DC 20590

Alternatively, it may be e-mailed to: pipeline.security@rspa.dot.gov

RSPA/OPS Follow-Up Actions:

RSPA/OPS intends to verify operators' measures to secure their critical pipeline facilities, beginning with operators of the pipelines that present significant risks to people and are most important to the integrity of the national energy infrastructure. RSPA/OPS will not ask operators to submit copies of their corporate security plans. Instead, RSPA/OPS and states will verify the plans on-site, and conduct checks in the field to determine whether each operator is implementing its plan as written and whether the plan is consistent with the security guidance published by the trade association for that operator's segment of the pipeline industry (see below). If the verification audit identifies security deficiencies, RSPA/OPS will work with the operator to correct them. RSPA/OPS will not maintain documentation about the contents of an operator's security program except to identify general deficiencies requiring correction. This documentation will not compromise the identity of critical facilities or the integrity of the security plan.

To assist RSPA/OPS in performing an on site security review, we request that an operator be prepared to discuss the following:

- a. a list of an operator's critical facilities;

- b. the steps which an operator would take to decrease the attractiveness of each critical facility as a target;
- c. procedures explaining how an operator would work with federal, state, and local agencies to respond to attacks on its critical facilities;
- d. an operator's process for conducting vulnerability assessments (if needed) of its critical facilities;
- e. cyber security methods for protecting its computer systems that are essential for the safe operation of the pipeline;
- f. procedures for training employees, including contractors, to respond appropriately during a security incident;
- g. procedures explaining how an operator would receive threat notification (physical attack, cyber attack, etc) and how it would disseminate this information to its employees, contractors, FBI, RSPA/OPS or other appropriate public officials;
- h. a process for controlling access to its facilities for both individuals and vehicles; (e.g. badging, visitor screening, vehicle searches);
- i. coordination with existing response plans, as necessary;
- j. how an operator would expedite restoration of service with minimal disruption (e.g. establishing a spare parts inventory, procedures for rerouting product to other lines);
- k. how the security plan conforms to the guidance developed by pipeline industry trade associations;
- l. procedures, if any, for conducting background checks on employees and/or contractors.

Industry Consensus Security Guidance:

In addition to the Pipeline Security Information Circular and Pipeline Security Contingency Planning Guidance, RSPA will use the following documents, which have been developed in concert with major industry groups, when evaluating operators' security plans. Hazardous liquid pipelines will be evaluated according to the American Petroleum Institute's "Guidelines for Developing and Implementing Security Plans for Petroleum Pipelines." Natural gas transmission and distribution pipelines, including liquefied natural gas facilities, will be evaluated according to the "Security Guidelines: Natural Gas Industry, Transmission and Distribution," developed by the American Gas Association and the Interstate Natural Gas Association of America. For operators that do not belong to a trade association, RSPA/OPS will provide the appropriate industry consensus security guidance documents to them upon request.

Protection of Operators' Security-Related Information:

RSPA/OPS recognizes that operators have concerns about our ability to protect operator security related information from disclosure. RSPA/OPS will withhold any security related information in our possession if it is sought under FOIA, as long as it is either: (1) commercial information that if released would likely cause an operator substantial competitive harm; or (2) related directly to the security of an operator's pipeline facilities.

Communicating Pipeline Security Information to Operators:

RSPA/OPS, the Department of Energy, and the FBI have systems in place to distribute security-related information to industry. Also, RSPA/OPS has established a recorded announcement at (202) 366-4532 that pipeline operators can call to check the latest threat condition for pipelines. At the time of publication of this notice, the nation is at the yellow alert level, as defined by the Office of Homeland Security. Any change in the nation's security posture will be reflected in the recorded announcement at that phone number.

If there is a change in the nation's security posture, RSPA/OPS expects operators to use good judgment in deciding what, if any, change in security measures are appropriate for their critical facilities.

The Office of Homeland Security has proposed a tiered system that corresponds to five threat levels:

Low = green

Guarded = blue

Elevated = yellow

High = orange

Severe = red.

For each threat condition, there are suggested protective measures that correspond to that threat level.

Dissemination of Guidance and Updating of Operator Contact Information:

RSPA/OPS is distributing the attached guidance document to pipeline operators, pipeline industry trade associations, regulatory and public safety agencies, and others with a demonstrated need to know. This document is not being made available to the general public because of its security-sensitive nature.

To update our distribution list for urgent security related information, RSPA/OPS asks that each operator e-mail the following information to: pipeline.security@rspa.dot.gov or mail this information to RSPA/OPS at the address provided above. RSPA/OPS is requesting 24-hour contact information for each operator's Chief Executive Officer, Chief Operating Officer and the person responsible for pipeline security. For each of these, we are requesting office, phone, and fax numbers, e-mail addresses, and, if applicable, cell phone and pager numbers. Alternatively, an operator with a 24-hour operations center may prefer to make that the recipient of urgent security-related information. In such cases, RSPA/OPS requests contact information for the operator's 24-hour operations center.

#