



## CHIEF COUNSEL AND PIPELINE SAFETY POLICY

### PHMSA FACILITY RESPONSE PLAN POLICY

**POLICY NUMBER: PHMSA 2050.1A**

#### U.S. DEPARTMENT OF TRANSPORTATION

#### PIPELINE AND HAZARDOUS MATERIALS SAFETY ADMINISTRATION

**ORIGINATING OFFICE:** Office of Chief Counsel and Office of Pipeline Safety Emergency Support and Security Division

**EFFECTIVE DATE:** June 27, 2014

---

Cynthia L. Quarterman  
Administrator, PHMSA

---

1. **PURPOSE.** To prescribe the policy on the types of information falling into the four categories of information protected under 49 U.S.C. § 60138 in oil spill response plans (“Facility Response Plan”).
2. **BACKGROUND.** In January 2012, the President signed Pub. Law 112-90, the Pipeline Safety, Regulatory Certainty, and Job Creation Act of 2011, codified at 49 U.S.C. § 60101 *et seq.* (“the Pipeline Safety Act”). Under the Freedom of Information Act, 5 U.S.C. § 552(b)(3) (Exemption 3) allows the withholding of information prohibited from disclosure by another federal statute. On April 24, 2013, the Office of General Counsel of the Department approved the use of 49 U.S.C. § 60138 of the Pipeline Safety Act as an Exemption 3 statute.

49 U.S.C. § 60138(a)(2) provides that the Secretary may, as he determines to be appropriate, exclude information from Facility Response Plans falling into the following categories:

- (A) proprietary information;
- (B) security-sensitive information, including information described in section 1520.5(a) of title 49, Code of Federal Regulations;
- (C) specific response resources and tactical resource deployment plans; and
- (D) the specific amount and location of worst case discharges (as defined in part 194 of title 49, Code of Federal Regulations), including the process by which an owner or operator determines the worst case discharge.

The authority to make the determination regarding the information in these categories to be protected from public disclosure has been delegated to PHMSA's Administrator.

3. **SCOPE**. Information to be excluded from public disclosure in Facility Response Plans.
4. **AUTHORITIES**.
  - a. Pub. Law 112-90, the Pipeline Safety, Regulatory Certainty, and Job Creation Act of 2011, codified at 49 U.S.C. § 60101 *et seq.*
  - b. 49 C.F.R. § 1.97(a)(1) and (10), Delegations to the PHMSA Administrator
  - c. The Freedom of Information Act, 5 U.S.C. § 552(b)(3), amended by Pub. Law 110-175 and Pub. Law 111-83.
5. **POLICY**. PHMSA will apply section 60138 (a) (2) (A) – (D) to the four categories of information as follows:

***a. Proprietary Information***

Section 60138 (a)(2)(A) of the Pipeline Safety Act authorizes the Secretary to withhold *proprietary information* from Facility Response Plans. PHMSA construes “proprietary” information in the Pipeline Safety Act as “trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential” information already protected from release under FOIA Exemption 4, 5 U.S.C. 552(b)(4). If a FOIA request is received for such information, PHMSA complies with DOT regulations in 49 CFR § 7.17 to consult with submitters of commercial and financial information if that information has been designated as confidential commercial information, or which DOT otherwise believes contains confidential commercial information.

Once the information is publicly-released by the submitter, it is no longer considered “proprietary.”

***b. Security–Sensitive Information***

Section 60138 (a)(2)(B) of the Pipeline Safety Act authorizes the Secretary to withhold *security-sensitive information* from Facility Response Plans, “including information described in section 1520.5(a) of title 49, Code of Federal Regulations,” from public disclosure.

Section 60138(a)(2)(B) includes information described in 49 CFR §1520.5(a), which are TSA's regulations on sensitive security information (“SSI”). (DOT's SSI regulations are found in 49 CFR Part 15). Section 1520.5(a) states that SSI is, “information obtained or developed in the conduct of security activities, including research and development, the disclosure of which, TSA has determined would –

- (1) Constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file);
- (2) Reveal trade secrets or privileged or confidential information obtained from any person; or
- (3) Be detrimental to the security of transportation.”

Sensitive Security Information in § 1520.5(a) is limited to “information obtained or developed in the conduct of security activities.” Security-sensitive information as set forth in section 60138 (a)(2)(B) of the Pipeline Safety Act *includes* the information described in § 1520.5. As such, security-sensitive information is broader than SSI.

PHMSA construes security-sensitive information as information in a Facility Response Plan that, if disclosed, would be of significant operational utility to a person(s) seeking to harm the pipeline infrastructure of the U.S., therefore adversely affecting transportation security. The following chart identifies security-sensitive information as points of vulnerability, i.e., a location, information about a weakness, or area in a pipeline system more susceptible to significant damage, or as information that could interfere with an operator’s ability to respond to a discharge of oil, i.e., reducing response resources or interfering with the deployment, direction, or coordination of response resources.

Using this standard, the following are the types of information that PHMSA believes could be used to target and damage pipeline infrastructure and will be withheld as *security-sensitive information* under 60138(a)(2)(B):

**Table of Information to be Redacted from Facility Response Plans as Security-Sensitive Information\*:**

Description of Information	Examples Included in Category	Examples Excluded from Category
1) Operational information pertaining to the safety and security of first responders and personnel.	Evacuation routes, first responder routes, rally points, and other detailed information pertaining to the location of personnel.	None
2) Any operational attribute or label of an above-ground pipeline facility shown on maps, illustration, in narrative, or in other media used by the plan.	Pump Station, Meter Station, Motor Valve, Guard Shack, Oil Separator	Company Name, emergency telephone numbers, non-operational or broad descriptions of the general “function” of a facility

3) Location of safety, security, and control systems and their components on maps, in narrative, or other media used by the plan.	Valves, Pressure Regulators, SCADA station, Control Center(s), Pump Station, Intrusion Detection sensors, fences, CCTV cameras, electrical generators, etc.	A facility's perimeter. General location (county/state) of response equipment.
4) Locations on maps, in narrative, or other media used by the plan, of high consequence areas <sup>1</sup> (HCAs).	Illustrations, including shaded areas or polygons, identifying high consequence areas. Description or boundaries of HCAs.	General topographic map features, city limits, elevation, most landmarks
5) Diagrams or functional descriptions of pipeline control systems, control system components, and communications/signaling systems used for pipeline control.	Schematic or other diagrams, blueprints, or portrayal or description of control system components and networks. Media and communications systems that can be used to connect these components.	General discussions that a control system exists.
6) Tank battery diagrams and facility piping configuration descriptions.	Maps, diagrams, pictures, or other portrayals of breakout tanks, tank batteries, containment systems, and piping configuration at a tank facility. Tank capacities. Containment system components and capacities. Tank worst case discharge amounts, calculations and locations.	Widely available maps or pictures of tank farm facilities (i.e., Google Map).
7) Security related information, which describes the continued physical security of an operator's facility, perimeter, employees, and surrounding population.	Threat scenarios, facility security and defense structures and procedures, and access control procedures used at facilities in an all hazards environment. Information describing the operator's coordination with government entities for security purposes also will be protected.	None. (Physical security information will be protected.)
8) Information pertaining to the operators continued information security and cyber security operations. This information will be withheld in support of Presidential Policy Directive 21 <sup>1</sup> .	Network configurations, control system equipment specifications, SCADA isolation times, and other information technology information that could be	None. (Cyber security information will be protected to ensure adversaries do not gain

<sup>1</sup> Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience

	used by an adversary to disrupt continued safe operations.	“insider” information.)
9) Values derived from the Worst Case Discharge amounts.	Response capacity values that can be used by an adversary to calculate the Worst Case Discharge.	Only values with a mathematical link back to the Worst Case Discharge will be redacted.

\* Notes: (1) “Security-Sensitive Information” will sometimes overlap with “Sensitive Security Information” (“SSI”) under 49 CFR Parts 15 and 1520. The DOT and DHS regulations at Parts 15 and 1520 mandate certain marking and handling measures for SSI, whereas the protection afforded under Section 60138 authorizes PHMSA to redact/withhold the information, including pursuant to a request submitted under the Freedom of Information Act (FOIA). Designation of information as Security-Sensitive Information under Section 60138 does not alleviate the obligation to mark and handle the information -- to the extent it also constitutes SSI -- in accordance with the DOT and DHS regulations at Parts 15 and 1520. (2) In the event that any “security-sensitive information” has been previously made public, PHMSA will consider the circumstances surrounding that prior disclosure in making its determination on whether such information should be redacted, taking into account then-current applicable laws and/or Government standards governing the treatment of previously-disclosed information.

***c. Specific Resources and Tactical Resource Deployment Plans***

49 U.S.C. § 60138(a)(2)(C) of the Pipeline Safety Act authorizes the Secretary to withhold *specific response resources and tactical resource deployment plans*.

At this time, PHMSA will not withhold information under section 60138(a)(2)(C), but may decide to do so in the future.

***d. Worst Case Discharge Information***

Section 60138(a)(2)(D) of the Pipeline Safety Act authorizes the Secretary to protect “the specific amount and location of worst case discharges” (as defined in part 194 of title 49, Code of Federal Regulations), including “the process by which an owner or operator determines the worst case discharge.”

The pipeline safety regulations (49 CFR § 194.105) require operators to calculate three types of worst case discharge – worst case discharge for pipeline, worst case discharge for breakout tank, and the worst case discharge amount based on the largest historic spill, if it exists. Operators calculate the worst case discharge for pipeline failures and breakout tank failures separately and then select the calculation with the largest volume for final worst case discharge determination.

PHMSA will also protect information that is inextricably linked to the worst case discharge as being part of the process by which the owner or operator determines the worst case discharge. The worst case discharge is a function of several variables which must be redacted to ensure an adversary cannot work backwards to calculate the worst case discharge. Additionally several of the variables include values that could help an outsider gain “insider information” on the type of safety/security devices used to ensure the continuity and safe operations of the pipeline infrastructure. Such “insider information” could be used by an adversary to increase the effectiveness of a cyber-attack or physical attack.

Therefore, PHMSA will protect the following information concerning worst case discharges:

Description of Information
1) Worst Case Discharge Amounts
2) Worst Case Discharge Location
3) Data inputs to methodology for calculating worst case discharge amounts, including values linked to isolation time, shutdown times, distance between valves, draindown attributes, breakout tank capacity, maximum release time, maximum flow rate, and other specific data used to calculate worst case discharge amounts.

---

<sup>i</sup> 49 CFR § 195.450 states that a high consequence area means: (1) a *commercially navigable waterway*, which means a waterway where a substantial likelihood of commercial navigation exists; (2) a *high population area*, which means an urbanized area, as defined and delineated by the Census Bureau, that contains 50,000 or more people and has a population density of at least 1,000 people per square mile; (3) an *other populated area*, which means a place as defined and delineated by the Census Bureau, that contains a concentrated population, such as an incorporated or unincorporated city, town, village or other designated residential or commercial area; and (4) an unusually sensitive area, as defined in § 195.6