

## Common Covered Task 001 Provide Security for Pipeline Facilities

### Directions

This training guide is to be used by a Veriforce Authorized Evaluator/Trainer and Trainee during on-the-job training (OJT) or prior to an evaluation as a resource. (S) Indicates a demonstration or skill task; (K) indicates a knowledge task.

### OJT Reminder

OJT is an active hands-on process. Practice should be as similar to the actual job task as possible. However, if the training is being provided on an actual job site while a covered task is actually being performed, the Evaluator either needs to be qualified on that covered task or be assisted by someone who is qualified on the covered task. The Evaluator should closely monitor the Trainee's practices to ensure safe and correct task performance. At no time should a non-qualified individual perform, or train for, a covered task unless directed and observed by a qualified individual. However, if the *"span of control"* for that particular covered task is "1:0" (requiring only qualified individuals to perform the covered task), the training must be simulated. Training is simulated by "walking through" the task and simulating all actual manipulations (valves, switches, tools, etc.) an individual would use during the performance of a covered task. Simulating includes the use of safety and administrative requirements as if the task were being performed live. Refer to the Veriforce Evaluator Training Program for more on how to conduct formal OJT.

### Disclaimer

This training resource is offered in good faith. Anyone choosing to utilize or rely on this training resource is doing so at their own discretion, risk and choice. Although every attempt has been made by Veriforce, LLC (the "Company") to ensure the correctness and suitability of this document and to correct any errors brought to the attention of the Company, the Company makes no representation or warranty regarding correctness or suitability (either directly or indirectly) of information referenced or implied within this training resource.

In no event shall the Company be liable for any damages (including, but not limited to, special, incidental or consequential damages) whatsoever (including, but not limited to, death, personal injury, damage to person or property, loss of use, and/or loss of revenues), whether in an action of contract, negligence, or other action, arising out of or in any way associated with the use or misuse of this document.

All critical information should be independently verified by the user and the user shall not rely on the contents provided herein without such independent verification. The subject matter included in this training has been compiled from a variety of sources and is subject to change without notice. The Company reserves the right to add, remove and alter information contained in this document without notice.

The Company may provide links to other sites for your convenience; however, the Company takes no responsibility and makes no representation or warranty regarding the accuracy or currency of information contained within such sites. The Company does not endorse any information, goods, or services referred to within such sites, and the provision of links by the Company shall not be interpreted to be an endorsement of such information, goods or services. The content of this training resource is provided for personal use only, and all other use, copying or reproduction of this training or website or any part of it is prohibited.

## Common Covered Task 001 Provide Security for Pipeline Facilities

### Recommended Student Training or Resources:

- DOT 49 CFR 195.436

### Introduction

America's energy system includes more than 2.6 million miles of pipeline across all fifty states. A disruption anywhere in the system can have a major impact on workers, companies, the public, and our environment.

It's not possible for us to provide the same types of protection to every part of the system, and we can't prevent some types of disruptions, such as natural disasters.

It is our responsibility, however, to provide protection against human threats. This responsibility is outlined on the federal level in 49 CFR 195.436.

There are many steps we can take to protect against man-made disruptions, whether they are malicious or unintentional.

Malicious incidents are the result of people intentionally trying to damage the pipeline or facility. This includes but is not limited to theft, vandalism, or terrorism.

Acts of terrorism are intended to intimidate, coerce, and disrupt the target population, usually for social or political reasons. It can be as complicated as hacking computer systems or as simple as a single person with an agenda, shooting at a pipeline.

While the reasons may differ, the effects of terrorism and vandalism can be the same. Whether the person shooting at the pipe is a terrorist or just intoxicated, a leak can be catastrophic.

While terrorism and certain acts of vandalism often have an obvious and immediate impact, theft and other types of vandalism can cost more than replacing or repairing damaged or stolen property. You may not discover the damage until it's too late.

Damage to important signs or markers can make it harder to locate and inspect facilities. Critical copper wiring or piping is at risk for theft, as well as fire extinguishers that might have prevented a small fire from growing.

Unintentional incidents can be just as harmful, whether it's unauthorized entry at a facility or encroachment on the line.

Trespassing can lead to time and money being wasted trying to ensure that unauthorized persons are not a threat.

Worse, if an unrelated incident such as an explosion or fire occurs, it would be hard to account for unauthorized people on the site, hurting disaster response efforts.

**Encroachment**, like trespassing, can put unauthorized people at risk if an incident occurs at the site. Unauthorized work activities, in particular, are more likely to cause major incidents.

Third-party excavation damage is responsible for more than three-quarters of fatalities and nearly half of injuries and evacuations occurring on pipeline systems. More than half of releases caused by third-party excavation damage involve people who don't use One Call and are unaware of the location of active pipelines.

Like trespassing, encroachment can make it harder for emergency services to access a site if an incident occurs.

Man-made incidents on the pipeline can have a catastrophic impact on employees, the public, and the environment. You play an important role in the security of our country's energy supplies.

This course will help you identify the threats facing pipelines and pipeline facilities, including breakout tank areas, pump stations, and other exposed facilities, and teach you more about what you can do to help protect our national resources.

**Knowledge:** Explain what is required prior to performing this task.

### **Pipeline Operator-Approved Procedures and Appropriate Equipment/Material**

Prior to performing this task, you will need to have the pipeline operator-approved procedures as well as the appropriate equipment and materials. The procedures will outline requirements for performing this task that are specific to the pipeline operator. Operators may also have specific requirements regarding the type of equipment that can be used to perform this task.

Therefore, it's important to follow the specific requirements of the procedures and only use operator-approved equipment. Doing so can ensure the task is performed correctly and according to the pipeline operator's standards.

**Knowledge:** Describe the steps to follow in providing protection for pipelines, pump stations, breakout tank areas, and other exposed facility equipment commensurate with the threat of a breach of security.

Pipeline security doesn't have a one-size-fits-all answer. There are certain methods, however, that we can use in a variety of places. Often, more than one method is required to secure a facility or piece of sensitive equipment.

Most of our pipeline infrastructure is protected, to some degree, by *redundancy* of lines and devices. This means we use back-up systems and devices that allow us to quickly shutdown or re-route damaged systems.

Besides back-up systems, there are many other methods used to control access to sensitive locations. These include, but are not limited to:

- Deterrents
- Monitoring
- Restricting access

Let's take a look at what each type of security includes. As we talk about them, keep in mind that just one method is usually not enough. We'll examine some ways they can be used together.

### **Deterrents**

Deterrents, such as warning signs, are one of the most common methods of pipeline protection. They are used to keep unauthorized people from accidentally entering pipeline areas or facilities.

Another noticeable deterrent on pipeline facilities, especially in more populated areas, is lighting. Processing facilities in particular keep all spaces well-lit for safety and security purposes.

If your facility uses deterrents, make sure that they're in good condition. All signs should be visible, legible, and spelled correctly. Report any damaged or faded signs or burnt-out lights.

### **Monitoring**

Depending on the type of facility, monitoring methods can range from the very simple to the incredibly high tech.

The simplest methods of monitoring are common even outside the oil and gas industry. These can include things such as perimeter or intruder alarms, video cameras, and security patrols or guards.

Signs of unauthorized access can also be checked for during right-of-way inspections and clearing.

Newer technologies tend to be used on pipeline and facilities that are in isolated but high-risk areas. These can include pressure sensors and fiber optic microphones that are capable of monitoring miles of pipeline that may be difficult to regularly patrol.

Air patrols, both manned and unmanned, can help ensure that unauthorized activity on the pipeline right-of-way is identified quickly and addressed.

We also use familiar technologies, such as SCADA systems, to help detect and isolate interference with pipeline or facilities.

If your role involves monitoring your work area or facility, make sure all communications and recording devices are in good condition. Post emergency contact information where all employees can access it.

If authorized to do so, make sure to follow the manufacturer's instructions when resetting, testing, or repairing monitoring equipment, such as cameras, alarms, and sensors.

Regular monitoring of breakout tank areas and pump stations, whether remote or by patrol, is *not* sufficient on its own. You must combine it with other methods of security, possibly including, but not limited to:

- Signs
- Fencing
- Locks

Be aware of your surroundings, and keep an eye out for signs of intrusion, such as missing or damaged equipment, suspicious packages, or unauthorized people on-site. Keep in mind that this can include landowners, hunters and fisherman, or other members of the public with no negative intent.

If you encounter these signs, contact your designated operator representative and follow operator procedures.

## **Restricting Access**

One of the most effective methods of restricting unauthorized access to pipelines is isolation. Most pipelines are buried or in areas that are hard to reach.

Although buildings are occasionally put up to protect these sites from the weather and intruders, many miles of pipeline and their accompanying facilities are practically inaccessible to non-employees.

Isolation is *not* enough protection for pipeline facilities, such as breakout tank areas, pump stations, or scraper traps. Other methods must also be used.

Perimeter fences and locked gates are common for sensitive worksites, and regularly-staffed sites may require ID badges. People may also be required to sign in with a gate guard or use access codes to enter automatic gates.

To prevent tampering, many pieces of equipment are located in buildings that can protect them.

Locks and chains are often used to secure equipment that may otherwise be easily manipulated, such as valves.

When working at a site with restricted access, make sure that all fences, chains, and locks are in good condition.

Check in any visitors you bring, according to company policy. All visitors should undergo a safety orientation and appropriate training before being allowed near pipeline or pipeline components.

The pipeline industry plays a huge role in the day-to-day lives of everyone in the United States, and maintaining the security of the industry is incredibly important.

Tampering with the pipeline by unauthorized people, whether malicious or unintentional, can lead to catastrophe. It is the responsibility of everyone on a worksite to pay attention to the signs of intrusion, and report any suspicious damage, items, or activities.

## Abnormal Operating Conditions (AOCs)

Candidates are required to possess the ability to **RECOGNIZE** and **REACT** to the listed AOCs for each task. Be prepared to answer questions concerning additional AOCs that may be relevant. Evaluators may ask questions about AOCs throughout the evaluation.

An AOC is defined in **49 CFR §§ 192.803** and **195.503** as:

A condition identified by the pipeline operator that may indicate a malfunction of a component or deviation from normal operations that may:

- Indicate a condition exceeding design limits; or
- Result in a hazard(s) to persons, property, or the environment.

---

**Recognize:** Unintentional releases, vapors, or hazardous atmosphere could be signs that an abnormal operating condition has occurred. Examples could include, but are not limited to:

- Blowing gas
- Puddles
- Dead vegetation

**React/Respond:** Proper reactions and/or responses to take in the event of an unintentional release, vapors, or hazardous atmosphere include the following:

- Eliminate potential ignition sources.
- Move to a safe location.
- Notify emergency response personnel, as appropriate.
- Notify the designated pipeline operator representative.

---

**Recognize:** An unintended fire and/or explosion on or near the pipeline is an abnormal operating condition.

**React/Respond:** Proper reactions/responses to take in the event of an unintended fire and/or explosion on or near the pipeline include the following:

- Move to a safe location.
- Notify emergency response personnel, as appropriate.
- Notify the designated pipeline operator representative.

---

**Recognize:** Evidence of sabotage or criminal activity is a sign of an abnormal operating condition. Examples could include, but are not limited to:

- Damaged pipeline components
- Damage or altered security systems, such as hasps, fences, locks, cameras, etc.
- Unauthorized person(s) on the facility or attempting to gain unauthorized access

**React/Respond:** Proper reactions/responses to take in the event of evidence of sabotage or criminal activity include the following:

- Secure area as required.
- Notify the designated pipeline operator representative.

---

**Recognize:** Failure or malfunction of pipeline security component(s) is an abnormal operating condition. Examples could include, but are not limited to:

- Malfunctioning or inoperative security systems

- Damaged fences

**React/Respond:** Proper reactions/responses to take in the event of a failure or malfunction of pipeline security component(s) include the following:

- Notify the designated pipeline operator representative.
- Secure area as required.

## Glossary

### **AOC**

abnormal operating condition

### **CCT**

common covered task

### **CFR**

Code of Federal Regulations

### **Encroachment**

corrosion with a length and width greater than three times the uncorroded wall thickness.

### **Redundancy**

corrosion with a length and width less than or equal to three times the uncorroded wall thickness.