PERMIAN BASIN
PETROLEUM ASSOCIATION

Recommended Oilfield Security Measures

for Upstream Operations

Compiled with the assistance of

VISTA ONE
STRATEGIC THREAT MITIGATION

October 2024

This document created by the Permian Basin Petroleum Association provides a set of recommended practices to combat oilfield crime, incorporating physical, cyber, and operational security measures alongside strategic recommendations for technology deployment and coordination with industry partners. Enhanced reporting protocols and structured training programs further solidify the approach, ensuring all personnel are equipped and informed to contribute to crime prevention and incident response. The measures included herein are not intended to be the only solutions that may be needed in combating oilfield crime but are intended to be a good beginning to address criminal activity and to protect your assets and employees.

Table of Contents

Physical Security Measures

Protecting an oil and gas field facility involves a combination of physical, cyber, and operational security measures. Here are some recommended practices for securing field assets:

1 Perimeter Security

- Install robust fencing, surveillance cameras, and motion detectors around the facility.
- Deploy cameras at strategic locations, particularly at the edges of target areas to maximize coverage. Consider using programmable game cameras or equivalent models. These cameras are cost-effective, easy to use, and can be programmed for motion alerts during specific hours, providing near real-time monitoring.

2 Camera Deployment

- Use programmable models that can alert relevant personnel during designated times.
- License Plate Reading (LPR) Cameras are rapidly evolving and becoming more accessible for private sector use. Consider evaluating emerging technologies for potential deployment.
- Leverage partnerships with other operators to maximize efficiency in camera positions and reduce costs.
- Install multiple cameras at high-value target locations, such as one camera to capture the rear of a vehicle for license plate identification and another to capture trucking company names and regulatory required numbers.

3 Locks & Valve Protection

- Ensure all gate locks are well-maintained and remain locked. Replace any cut or removed locks immediately. Change combinations periodically to prevent unauthorized access.
- Exposed locks on valves are vulnerable to tampering and cutting by theft subjects. Consider installing lock guards on valves that cannot be secured via plug.
- Valve plug options are an excellent solution where feasible.

4 Lighting

- Adequate lighting is a statistically significant deterrent to unauthorized access. Place lights in strategic locations to illuminate target areas and observation points near highways or heavily traveled roads. This can interfere with the use of night vision equipment by potential theft scouts and improve visibility for security personnel.

5 Security Guard Services

- Security guards provide a visible deterrent but may not be sustainable long-term. Consider the following deployment strategies:
    - High Visibility Roving Patrols: Ensure theft deterrence across the area.
    - Low Visibility Stationary Observation: Place guards at vantage points to conduct “observe and report” activities. Stationary observation may transition to moving surveillance if required until law enforcement can intervene.

6 Copper Theft Recommendations

- Copper wiring is a frequent target for theft due to its high resale value. By replacing stolen copper wire with aluminum wire equivalents, operators can reduce the attractiveness of the material to thieves without compromising functionality. Aluminum wire provides similar electrical conductivity and durability but has a significantly lower market value.
- Electric submersible pumps (ESPs) are critical assets that are often targeted for their copper wiring and components. Installing an audible and visible strobe alarm on a pole near each ESP that activates when power is cut or disrupted serves as both a deterrent to theft and an immediate alert system for nearby personnel and security responders.

Cybersecurity Measures

1 Network Security

- Use firewalls, intrusion detection systems, and secure communication protocols to protect the facility's network from cyber threats.

2 Data Backup & Recovery

- Establish a secure data backup and recovery process to protect against data loss in the event of a cyber incident. Regularly test backups to ensure data integrity and availability.

3 Regular Updates

- Keep all software and systems updated to protect against vulnerabilities and cyber-attacks.

4 Access Control

- Implement strict access control measures, including multi-factor authentication (MFA) and role-based permissions, to ensure only authorized personnel have access to sensitive data and systems.

5 Employee Training

- Conduct regular cybersecurity training for employees to recognize and respond to cyber threats.

6 Incident Response Plan

- Develop and regularly update an incident response plan to quickly address any cyber incidents.

7 Cybersecurity Assessment

- To ensure the ongoing security of your organization's systems and data, we strongly recommend implementing a program of regular cybersecurity assessments and services by a vendor separate from Information Technology providers. In today's dynamic threat landscape, where cyberattacks are becoming increasingly sophisticated, these assessments are essential to maintain a robust security posture and ensure business continuity. By proactively identifying and mitigating vulnerabilities, you can minimize the risk of disruptions and downtime caused by cyberattacks. These assessments also provide valuable insights into your security posture, enabling continuous improvement and strengthening of your defenses.

Reporting & Incident Response

The reporting and documentation of any incident are crucial for successful investigation and resolution. Immediate and accurate communication with local law enforcement is essential to ensure that proper procedures are followed, and that all relevant information is captured.

1 Law Enforcement Coordination

- Any theft of product, materials, or equipment must be reported immediately to local law enforcement. While telephone reporting is acceptable, in-person reporting is preferred to facilitate evidence collection and scene documentation. Initiate contact by clearly stating the purpose of the call is to report a theft and insist that a report be made at the incident location. If in-person and telephone reporting are not available options, submit a written reporting to the appropriate law enforcement agency. A list of law enforcement agencies in the Permian Basin can be found at the end of this full set of recommendations.

2 Documentation Protocols

- Ensure that the following details are provided to the responding officer:
  - GPS coordinates, victim information, loss data (amounts and value), time, and witness information. (An account of who, what, where, when, why, and how.)
  - Collection of any physical evidence remaining at the scene (e.g., cut locks, tools, suspect litter).
  - Collection and submission of any latent evidence (e.g., fingerprints, DNA, cut locks with tool marks) to a laboratory for analysis.
  - Photographs with scale or cast tire and shoe impressions, evidence in place, and the overall crime scene.
  - Identify as clearly as possible the items that appear to have been stolen or damaged (i.e. number of barrels of crude oil, trailer and pump with trailer registration information and all serial numbers, color, make model, etc., or number of pipe joints and size of pipe).
- Obtain the reporting officer's name and incident report number for record-keeping and follow-up.

Training & Awareness Programs

To ensure a cohesive approach to crime prevention and incident response, it is recommended that the information provided in this report be integrated into a comprehensive training program for all personnel.

1 Personnel Training

- Develop training modules that address theft awareness, incident reporting, cybersecurity protocols, and coordinated response procedures.
- Conduct periodic drills and scenario-based training to evaluate response efficiency and identify areas for improvement.

2 Employee Awareness

- Promote awareness among employees regarding common theft methods and potential insider threats.
- Encourage reporting of suspicious activities and provide a confidential channel for such communications.

Operational Security Measures

1 Schedule Management

- Where possible, schedule all liquids pickup from remote facilities during daylight hours only. Communicate these schedules with local law enforcement to assist in identifying unauthorized access during off-hours.

2 Digital Transmission Systems

- Transition liquids transmission tickets to a digital system, as paper tickets have become a target for counterfeiting.

3 Risk Assessments

- Conduct regular assessments to identify and mitigate potential security vulnerabilities.

4 Emergency Preparedness

- Develop and practice emergency response plans for scenarios such as fires, spills, and natural disasters.

5 Safety Protocols

- Implement strict safety protocols to prevent accidents and ensure the well-being of employees.

6 Equipment Maintenance

- Regularly maintain and inspect equipment to prevent failures and ensure operational integrity.

Additional Measures

1 Asset Tracking

- Use GPS and RFID technology to track the location of mobile and fixed assets.

2 Lone Worker Safety

- Implement safety measures for lone workers, such as wearable devices that can alert emergency services if needed.

3 Mitigation of Insider Threat

- Implement inventory control systems and procedures, as well as quarterly or yearly audits to deter employee theft.
- Utilize overt and concealed security cameras at critical locations to identify employees involved in theft.
- Monitor employee use of company purchasing cards to deter theft of services. Strict guidelines and internal training on allowable purchases may also deter misuse.
- Implement strict policies on data and electronics use to safeguard sensitive information.

4 Vendor Vetting

- In today's rapidly evolving landscape, implementing a robust vendor vetting and audit program is essential for oil and gas operators to maintain compliance, minimize risks, and enhance operational efficiency. A structured vendor vetting and audit process ensures that all oilfield service providers align with the operator's standards and regulatory requirements. This proactive approach mitigates the risk of operational disruptions, costly compliance breaches, and reputational damage by establishing consistent and reliable service quality. By thoroughly evaluating and regularly auditing vendors, operators can build a resilient supply chain, foster transparency, and ultimately protect their financial assets and stakeholders.