TSA Cyber Security Directives and Impacts on the Natural Gas Industry

Brian Lenhart
Group Leader, Gas CRM Engineering

TSA Pipeline Security Authority

Colonial Pipeline Cyber Incident

TSA Security Directives

Impact to Operations

What’s Next?

TSA Pipeline Security Authority

The TSA has primary oversight responsibility for both the physical security and cybersecurity of transmission and distribution pipeline systems, stemming from when the TSA was formed after the terrorist attacks on September 11th.

In response to the 9/11 Commission Act of 2007, the TSA's Pipeline Security Branch issued voluntary Pipeline Security Guidelines in 2011.

- The Pipeline Security Branch released revised guidelines in March 2018, and Change 1 in April 2021.

U.S. DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

TSA Pipeline Security Authority

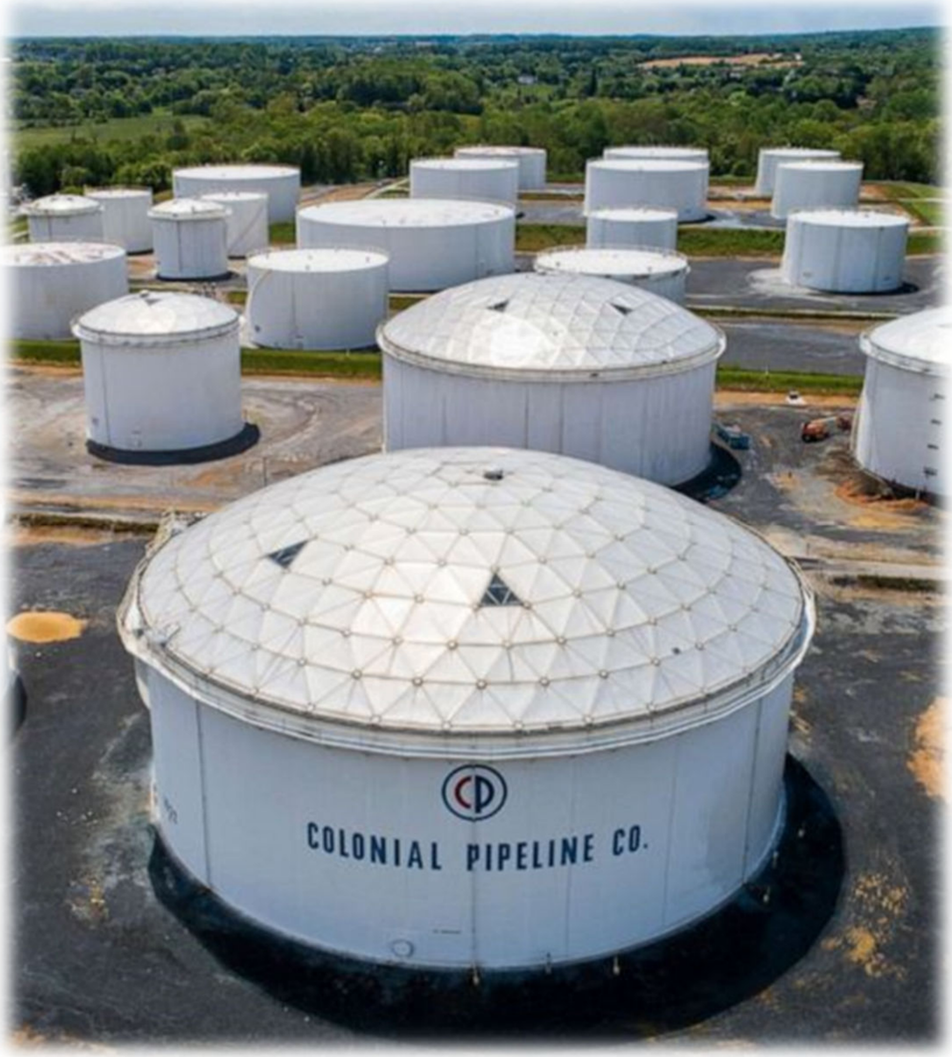
Pipeline Security Guidelines

The Pipeline Security Guidelines provided direction for operators to voluntarily develop a risk-based corporate security program to address and document the organization’s policies and procedures for managing physical and cyber security related threats, incidents, and responses.

The TSA’s Pipeline Security Branch also is responsible for identifying the Top 100 critical pipeline systems in the nation.

- Additionally, the Pipeline Security Branch is responsible for conducting voluntary security reviews, which access the extent to which these 100 pipelines systems are following the intent of TSA’s Pipeline Security Guidelines.

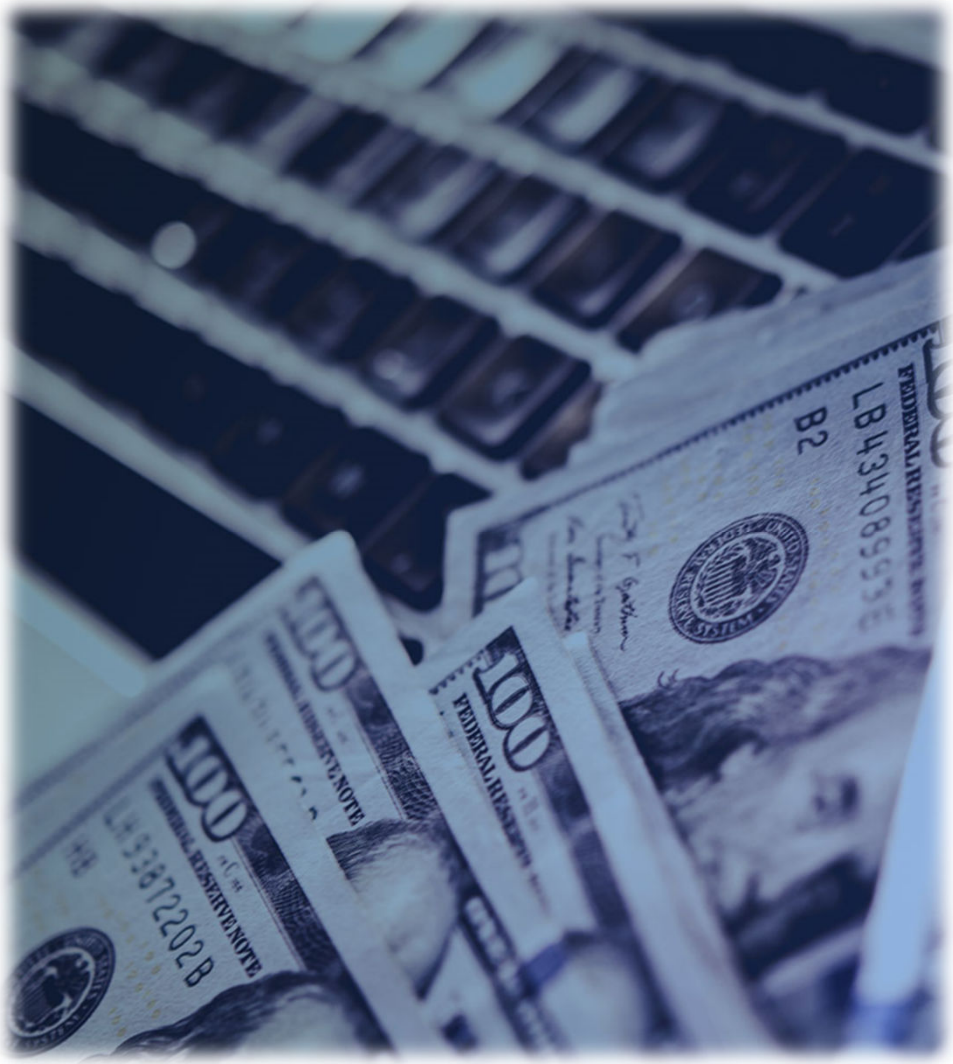
Colonial Pipeline Cyber Incident



On May 7, 2021, Colonial Pipeline was the victim of a ransomware attack perpetrated by the Russian criminal hacking syndicate, Darkside.

While OT systems were not immediately impacted, Colonial proactively shut down pipeline operations, fearing that the attackers may have also been able to gain access to information that would allow them to carry out further attacks.

Colonial Pipeline Cyber Incident



Darkside was able to gain access to Colonial’s systems via an exposed password for an employee’s VPN account.

Colonial paid the hacker’s ransom of ~$4.5 million within hours of the attack.

Pipeline operations were restarted on May 12th, and were fully restored on May 13th.

TSA Security Directives

Security Directive Pipeline-2021-01

In response to the Colonial Pipeline cyber incident, and other imminent cyber threats, the TSA issued the first Security Directive on May 28, 2021.

Security Directive-01 requires three actions;

1. TSA-specified owner/operators must report cybersecurity incidents to CISA.
2. Owner/operators must designate a Cybersecurity Coordinator who is required to be available to TSA and CISA 24/7.
3. Owner/operators must review current cybersecurity activities against the TSA's Pipeline Security Guidelines Section 7 to address cyber risk, identify any gaps, develop remediation measures, and report the results to the TSA.

Only the top 100 critical pipeline system owners were required to comply.

TSA Security Directives

Security Directive Pipeline-2021-02

On June 19, citing “ongoing cybersecurity threats to pipeline systems” the TSA, in consultation with CISA, DOE, PHMSA, and the DOT, issued Security Directive-02 to complement the initial requirements of Security Directive-01. Security Directive-02 was effective as of July 26, 2021.

Security Directive-02 requires three additional actions;

1. Implementation of mitigation measures to reduce the risk of compromise from a cyberattack.
2. Development of a Cybersecurity Contingency/Response Plan to reduce the risk of operational disruption or functional degradation of necessary capacity should IT or OT systems be affected by a cybersecurity incident.
3. Test the effectiveness of the Owner/Operators cybersecurity practices through an annual cybersecurity architecture design review.

TSA Security Directives

Security Directive Pipeline-2021-02C

On July 27, 2022, the TSA issued Security Directive-02C, which superseded 02B. The revised directive was intended to provide pipeline operators with more flexibility to meet the TSA's desired security outcomes for the industry than the prescriptive requirements of the previous directive.

Security Directive-02C has three mandates;

1. Establish a TSA approved Cybersecurity Implementation Plan.
2. Develop and maintain a Cybersecurity Incident Response Plan
3. Establish a Cybersecurity Assessment Program.

TSA Security Directives

Security Directive Pipeline-2021-02C

The Operator's Cybersecurity Implementation Plan must address the following;

A. Identify Operator's critical cyber systems

B. Implement network segmentation polices and controls

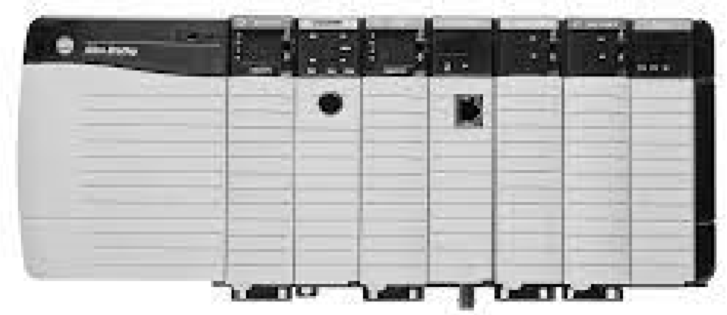
C. Implement access control measures

D. Implement continuous monitoring and detection policies

E. Reduce the risk of risk of exploitation of unpatched systems through application of security patches and updates

Impacts on Operations in the Field
Informational Technology

Impacts on Operations in the Field
Operational Technology



Advanced Notice of Proposed Rule Making

On November 30, 2022, the TSA published an ANPRM “Enhancing Surface Cyber Risk Management” in the Federal Register. The proposed rule would impact Pipeline and Rail (freight, passenger, and transit).

In the proposal’s background, the TSA states

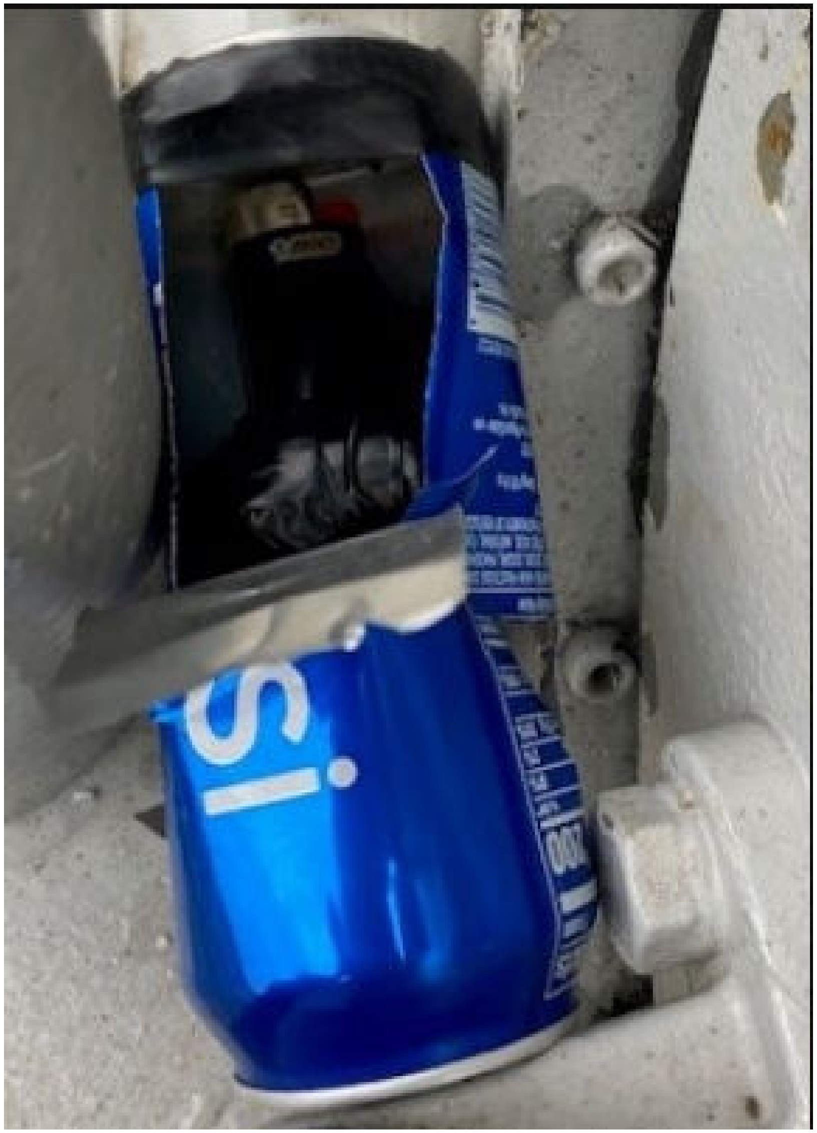
> *“As pipeline and rail owner/operators begin integrating IT and OT systems into their ICS environment to further improve safety, enable efficiencies, and/or increase automation, the ICS environment increasingly becomes more vulnerable to new and evolving cyber threats. A successful cyber-intrusion could affect the safe operation and reliability of OT systems, including SCADA systems, process control systems, distributed control systems, safety control systems, measurement systems, and telemetry systems.”*

Potential Physical Security Concerns

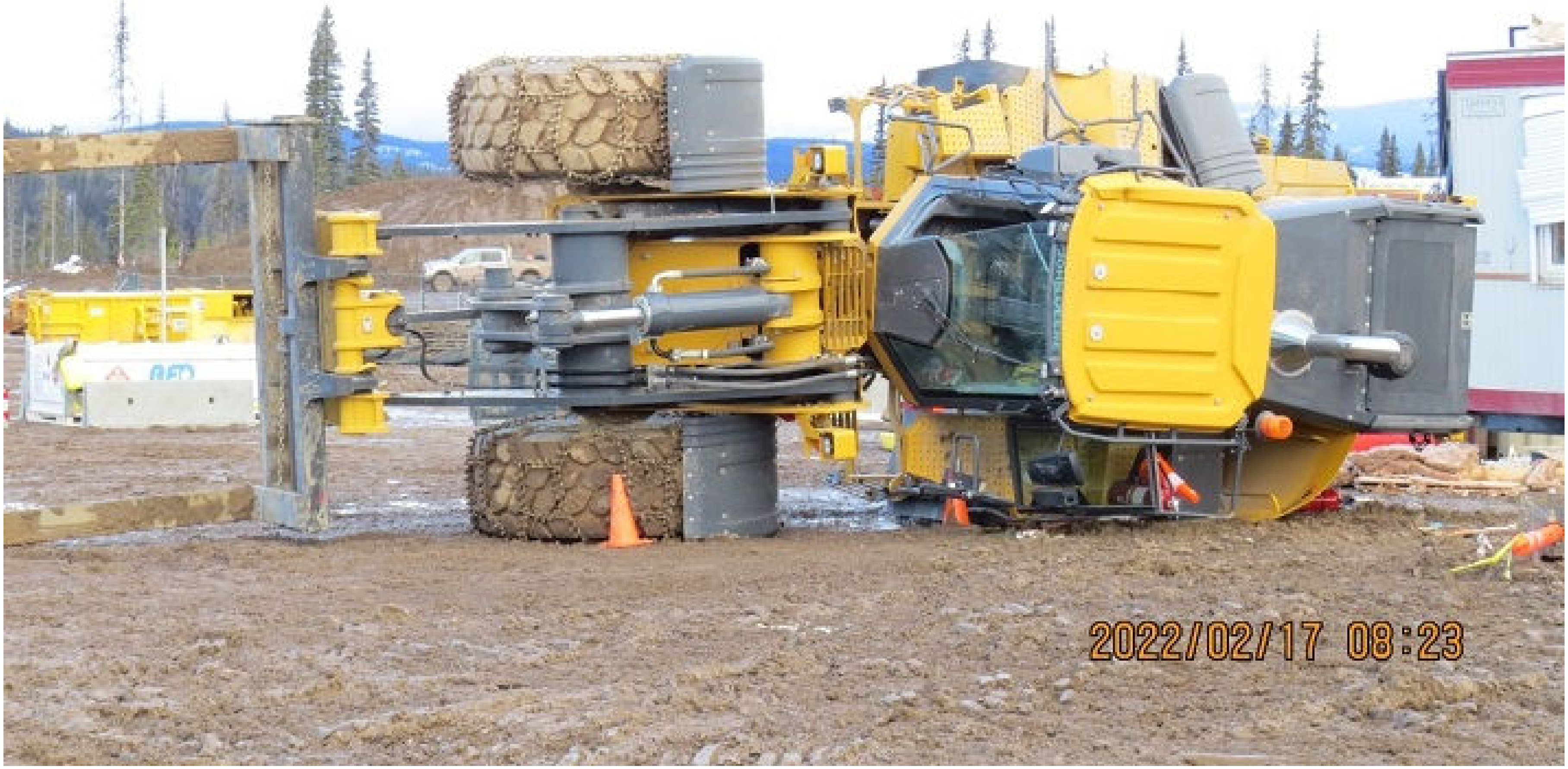
Over recent years, physical security concerns have been realized, as attacks on natural gas and electric infrastructure have been executed throughout North America.

Arson Fire at Regulator Station Continuous Bleed Vent

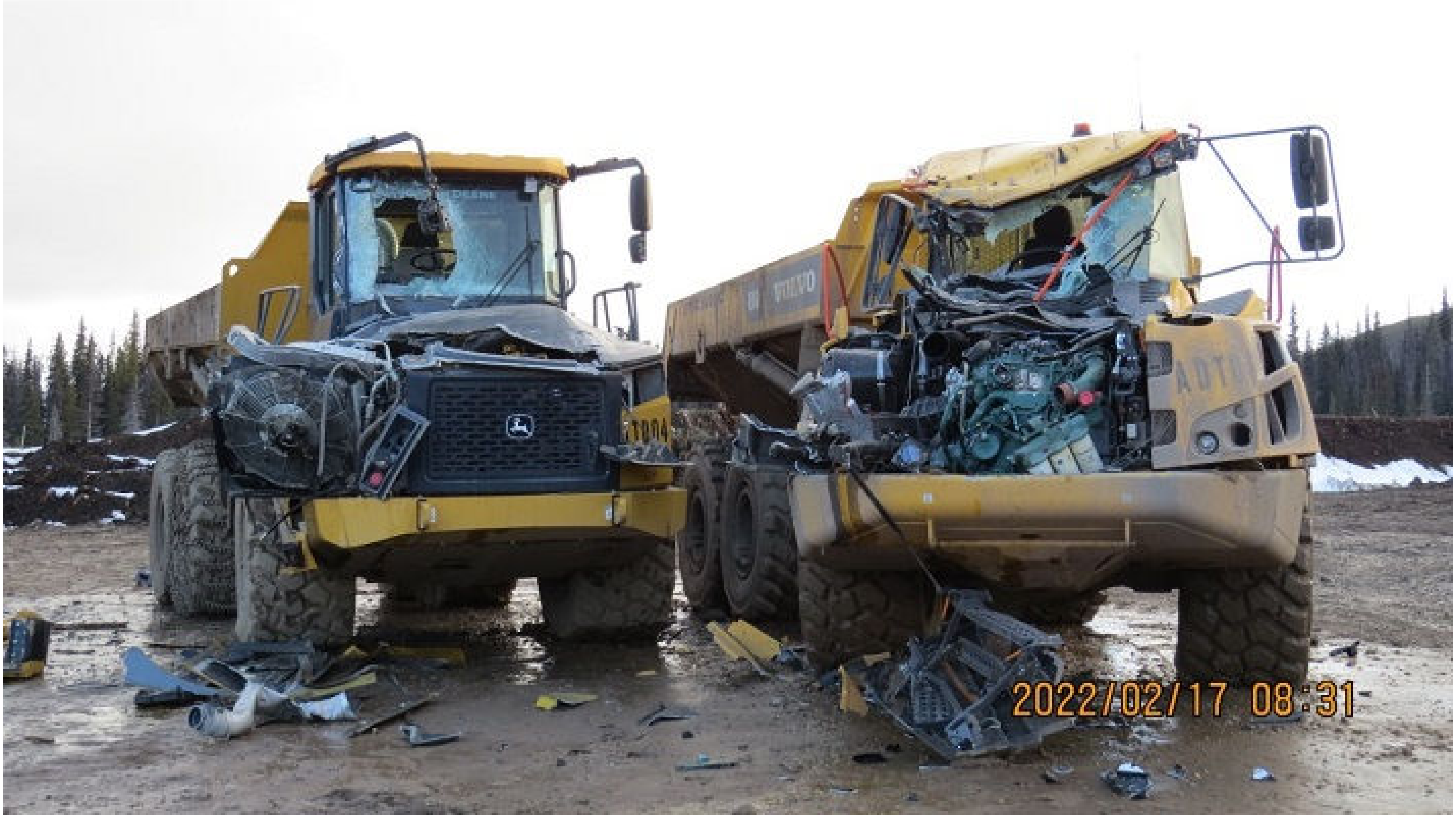
Improvised Device Found at SW PA Facility



Marten Forest Service Road



Marten Forest Service Road



Physical Security Compliance?

While not required by regulation or directive today, physical security requirements could follow a significant physical security event, just as the TSA Security Directives followed the Colonial Pipeline Cyber Incident. The TSA Pipeline Security Guidelines provide a good foundation for physical security.

Fencing

Gates

Lighting

Personal Identification

Equipment Inspection

Access Controls

Lock and Key Control

Intrusion Detection

Background Investigation

Design and Construction