

FEDERAL BUREAU OF INVESTIGATION

OFFICE OF PARTNER ENGAGEMENT

PUBLIC SAFETY AWARENESS REPORT



(U) PREPARED BY THE FBI OFFICE OF PARTNER ENGAGEMENT,
WEAPONS OF MASS DESTRUCTION DIRECTORATE

6 APRIL 2023
[OPE-23-SA-009]



(U) This document is classified: UNCLASSIFIED//FOR OFFICIAL USE ONLY.

(U) Public Safety Awareness Report template approved for fiscal year 2023, as of 1 OCTOBER 2022.

(U) Please direct comments and queries regarding this product to the FBI Office of Partner Engagement's Enhanced Engagement Unit at OPE-EEU@fbi.gov.

(U) This product expresses the judgments and perspective of this office and may not reflect the national perspective of the Federal Bureau of Investigation.

(U//FOUO) Heightened Threat Activity Surrounding Oil and Gas Infrastructure Possible Following Film Release

(U) SITUATIONAL AWARENESS

(U//FOUO) In light of the upcoming release of the film, "How to Blow Up a Pipeline," the FBI is providing situational awareness to inform and prepare partners for a possible increase in threat activity and reporting surrounding oil and gas infrastructure, particularly pipelines. The film has potential to inspire threat actors to target oil and gas infrastructure with explosives or other destructive devices.

- (U) The full-length film "How to Blow Up a Pipeline," which will be released in theaters on 7 April 2023, tells the story of a group of individuals who plan to target an oil pipeline in West Texas. The film is based on a book of the same name, which advocated for sabotage against the fossil fuel industry to prevent the ecological destruction of the planet.^{1,2}
- (U) As of 2021, according to the American Petroleum Institute website, there were approximately 2.4 million miles of natural gas pipelines and 190,000 miles of liquid petroleum pipelines in the United States, most of which was underground.³
- (U) Reporting since 2021 indicates threat actors have been increasingly targeting infrastructure sites and equipment in the Energy Sector. Such targeting to date has focused primarily on electrical transmission and distribution substations, coolant components, and equipment, as opposed to oil and gas pipelines and infrastructure.⁴

(U) CONSIDERATIONS

(U) If your agency has information that may assist in identifying suspects engaged in criminal activity or preventing such activity, please contact the FBI.

(U) Any information regarding suspected criminal activity should be reported to your nearest FBI Field Office: <https://www.fbi.gov/contact-us>; or report any leads, threats, and suspected criminal activity: <https://tips.fbi.gov/>. Additionally, we encourage law enforcement use of eGuardian, which is accessible via the Law Enforcement Enterprise Portal (LEEP): <https://www.cjis.gov/>. If the information is urgent in nature, then please contact your local FBI field office directly and follow up with an eGuardian report.

(U) An indicator alone does not accurately determine the likelihood of criminal activity against oil and gas infrastructure; security and law enforcement personnel should evaluate the totality of behavior and circumstances.

(U) The following suspicious activities/indicators include, but are not limited to, any individual, group, or business; observe these indicators in context and not individually:

- (U) Explicit reconnaissance or surveillance activity of oil and gas pipelines, refineries, and related facilities and equipment.
 - (U) Discreet or unusual use of cameras or video recorders, sketching, or note-taking aimed at learning about infrastructure operations.
 - (U) Suspicious questioning of security personnel and employees of facilities, including questions regarding hours of operation and access points.
 - (U) Unusual observation of security personnel's reaction procedures during drills or following fictitious emergency telephone calls to the same locations or similar venues.
 - (U) Repeatedly loitering around, initiating false alarms, or conducting fictitious emergency calls to oil and gas facilities.
 - (U) Attempts to breach security at oil and gas facilities by disguising as workers at the site.
 - (U) Theft of equipment from oil and gas facilities, including tools, employee uniforms and identification cards, and keys to access points.
- (U) Signs of tampering and/or unauthorized access to easily accessible critical infrastructure sites.

(U) RESOURCES

- (U) Federal, state, local, tribal, and territorial, intelligence, law enforcement, and homeland security partners may refer to the following resources and guidelines to prepare for and mitigate threat activity against oil and gas and other energy infrastructure:
 - (U) Joint Counterterrorism Assessment Team (JCAT) First Responder's Toolboxes:¹
 - (U) Complex Operating Environment—Oil and Gas Pipelines
 - (U) Complex Operating Environment—Oil and Natural Gas Refineries
 - (U) Complex Operating Environment—Electric Grid
 - (U) Reporting Suspicious Activity—Critical for Terrorism Prevention

(U) These and other JCAT First Responder Toolboxes can be accessed and retrieved at <https://www.dni.gov/index.php/nctc-how-we-work/joint-ct-assessment-team/first-responder-toolbox>.

- (U) FBI Public Safety Awareness Report: Threat Actors Targeting US Electrical Grid²

(U) THE INFORMATION IN THIS PUBLIC SAFETY AWARENESS REPORT (PSAR) PREPARED BY THE FBI OFFICE OF PARTNER ENGAGEMENT AND WEAPONS OF MASS DESTRUCTION DIRECTORATE, IS PROVIDED TO ENHANCE PUBLIC SAFETY AND FOR SITUATIONAL AWARENESS PURPOSES ONLY. NO INFORMATION CONTAINED IN THIS PSAR, NOR ANY INFORMATION DERIVED THEREFROM, MAY BE USED IN ANY PROCEEDING (WHETHER CRIMINAL OR CIVIL), TO INCLUDE ANY TRIAL, HEARING, OR OTHER PROCEEDING BEFORE ANY COURT, DEPARTMENT, AGENCY, REGULATORY BODY, OR OTHER AUTHORITY OF THE UNITED STATES WITHOUT PRIOR APPROVAL FROM THE FBI. THESE RESTRICTIONS APPLY TO ANY INFORMATION EXTRACTED FROM THIS DOCUMENT AND USED IN DERIVATIVE PUBLICATIONS OR BRIEFINGS.

To report any leads, threats, and suspected criminal activity, please visit <https://www.fbi.gov/tips> or contact your local FBI Office: <https://www.fbi.gov/contact-us>.

²(U) For more information on this PSAR, please use LEEP/JusticeConnect - [LESC-FBI-IIP](#).

(U) ENDNOTES
