Technology Security and Protection of America’s Pipeline Energy Grid

Austin Gould – Assistant Administrator
Requirements & Capabilities Analysis

November 14th 2023

Dubai Skyline

Dubai Airshow

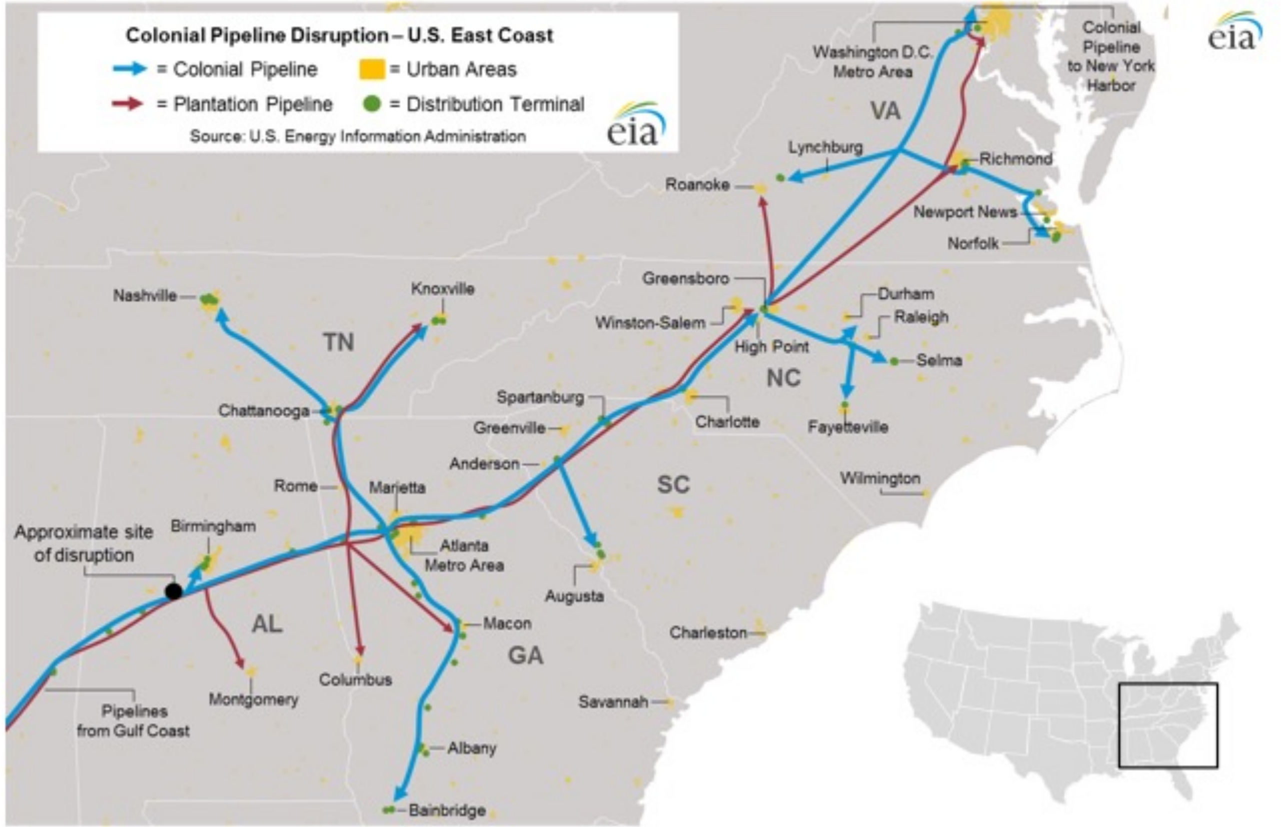
DUBAI AIRSHOW
WELCOME TO THE DUBAI AIRSHOW 2021
#DUBAI AIRSHOW
THE FUTURE OF THE AEROSPACE INDUSTRY

Transportation Security Administration (TSA)

Mission: Protect the nation’s transportation systems to ensure freedom of movement for people and commerce

Diverse mission to include not only civil aviation but pipeline, railroad, multimodal public area capabilities

Colonial Pipeline Ransomware Attack



By U.S. Energy Information Administration - Colonial Pipeline Disruption U.S. East Coast, Public Domain

May 7th, 2021

The **Colonial Pipeline**, an American oil pipeline system that originates in Houston, Texas, suffered a ransomware cyberattack that impacted computerized equipment.

It is 5,500 miles long and can carry 3 million barrels of fuel between Texas and New York daily, making it critical to U.S fuel supply, transportation, and economy

TSA Cybersecurity Security Directives

First Directive: May 27, 2021

Operators are required to review current practices to assess cyber risks and report the results to TSA and CISA no more than 12 hours after an incident is identified

Required owners and operators of critical pipelines to designate a Cybersecurity Coordinator who must be available to TSA and CISA 24-hours a day, 7 days a week

SD-02 Series

Outcome Focused Compliance

Developed extensive input from industry stakeholders and federal partners including CISA

Security directive takes an innovative, performance-based approach to enhancing security, allow industry to leverage new technologies and be more adaptive to changing environments

SD-02D Series

Establish and implement a TSA-approved Cybersecurity Implementation Plan

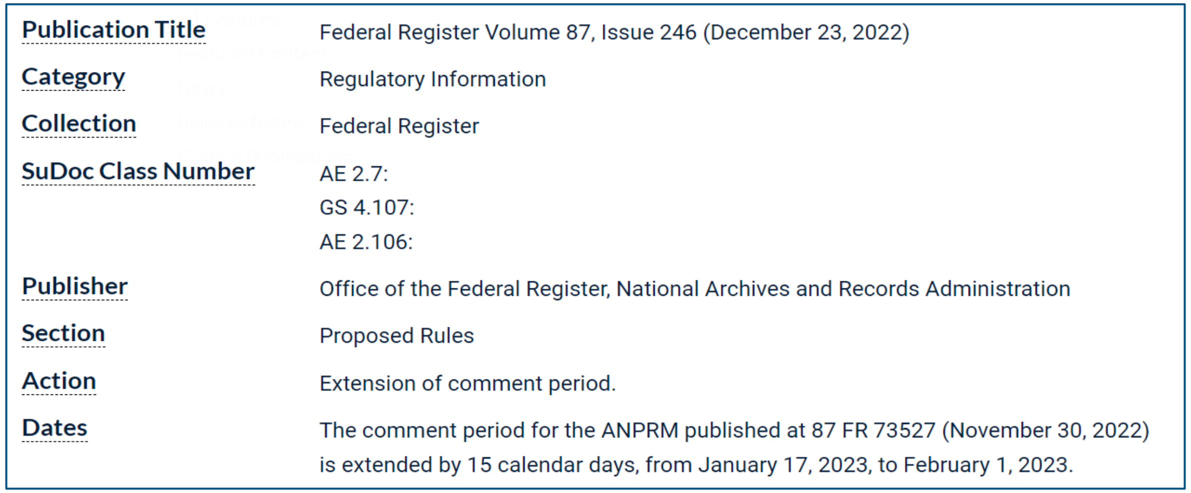
Develop and maintain a Cybersecurity Incident Response Plan to reduce the risk of operational disruption

Establish a Cybersecurity Assessment Plan to assess effectiveness of cybersecurity measures and is submitted annually by the Owner/Operator for TSA review and approval

Evolution of Security Directives

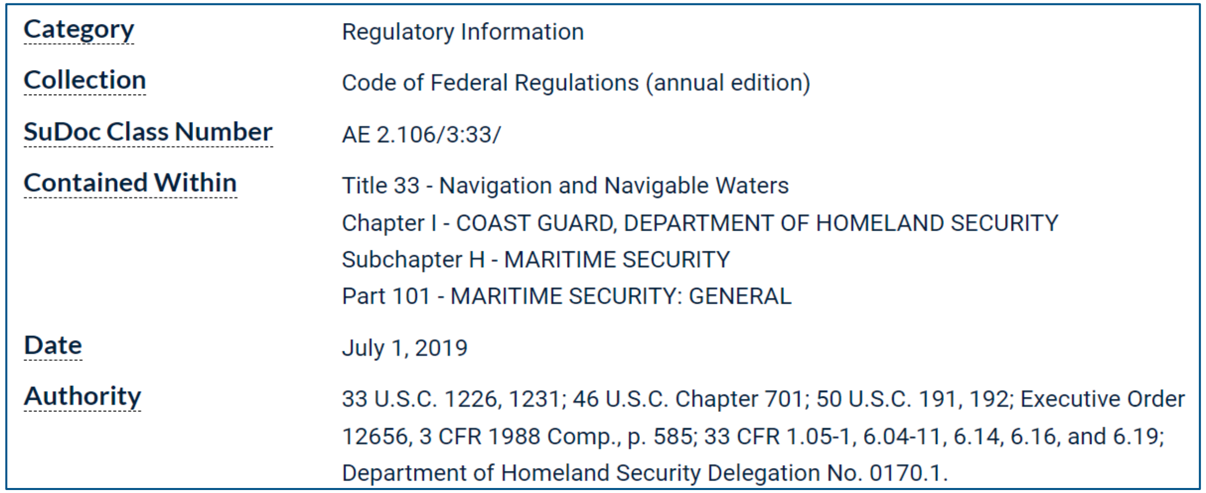
Rulemaking Process

TSA Rulemaking



Publication Title	Federal Register Volume 87, Issue 246 (December 23, 2022)
Category	Regulatory Information
Collection	Federal Register
SuDoc Class Number	AE 2.7: GS 4.107: AE 2.106:
Publisher	Office of the Federal Register, National Archives and Records Administration
Section	Proposed Rules
Action	Extension of comment period.
Dates	The comment period for the ANPRM published at 87 FR 73527 (November 30, 2022) is extended by 15 calendar days, from January 17, 2023, to February 1, 2023.

USCG Rulemaking



Category	Regulatory Information
Collection	Code of Federal Regulations (annual edition)
SuDoc Class Number	AE 2.106/3:33/
Contained Within	Title 33 - Navigation and Navigable Waters Chapter I - COAST GUARD, DEPARTMENT OF HOMELAND SECURITY Subchapter H - MARITIME SECURITY Part 101 - MARITIME SECURITY: GENERAL
Date	July 1, 2019
Authority	33 U.S.C. 1226, 1231; 46 U.S.C. Chapter 701; 50 U.S.C. 191, 192; Executive Order 12656, 3 CFR 1988 Comp., p. 585; 33 CFR 1.05-1, 6.04-11, 6.14, 6.16, and 6.19; Department of Homeland Security Delegation No. 0170.1.

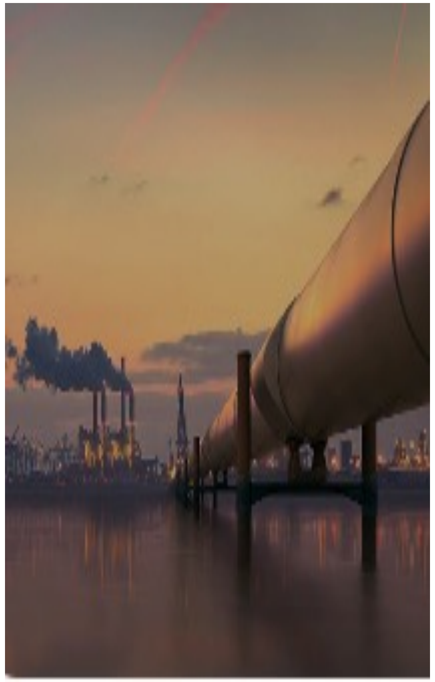
On November 30, 2022, TSA released an advanced notice of proposed rulemaking that sought input regarding ways to strengthen cybersecurity and resiliency in the pipeline and rail (including freight, passenger, and transit rail) sectors.

On January 17th, 2023, comments closed to the Federal Docket Management System (FDMS), a government-wide electronic docket management system.

The USCG proposes to update its maritime security regulations by adding cybersecurity requirements to existing Maritime Security regulations in 33 CFR part 101 et seq. This proposed rulemaking is part of an ongoing effort to address emerging cybersecurity risks and threats to maritime security by including additional security requirements to safeguard the marine transportation system.

What is next?

What We’re Doing Now



Aviation, Rail, and Pipeline

What is Next

Continue to collaborate with other government agencies

Risk Assessments

Cybersecurity training

Continuous monitoring

Sector Risk Management Agencies

The Department of Homeland Security (DHS) and the Department of Transportation (DOT) are designated as the Co-Sector Risk Management Agencies for the Transportation Systems Sector with TSA and USCG serving as the delegated leads for DHS. To build cybersecurity resilience in partnership between DHS and DOT, the following co-SRMA priorities have been identified.

- *Develop and implement risk-based process to incorporate TSA cybersecurity requirements into DOT infrastructure discretionary grant programs*
- *Conduct joint outreach across modes based on risk prioritization to enhance awareness of cyber threats, cybersecurity best practices, federal services and grants*
- *Pursue public-private partnership projects to enhance cyber resilience through efforts including vulnerability testing and incident response planning*
- *Develop risk registers by mode, drawing from ongoing vulnerability and threat assessments, in order to assess relative risk and prioritize future efforts*

Additional Questions/Comments

Point of Contact

Austin Gould
Assistant Administrator
Requirements and Capabilities Analysis (RCA)
Transportation Security Administration (TSA)
Department of Homeland Security (DHS)
Austin.Gould@tsa.dhs.gov

TRANSPORTATION SECURITY ADMINISTRATION