February 1, 2023

D.O.T. Docket Management System

TSA Docket No. TSA–2022–0001
U.S. D.O.T. Docket Operations Facility (W12-140)
West Building, 1200 New Jersey Avenue SE,
Washington, DC 20590-0001

Re: Enhancing Surface Cyber Risk Management; Transportation Security Administration, 49 C.F.R. Chapter XII, Docket No. TSA–2022–0001, Comments of the Fiber Optic Sensing Association.[i]

Dear Administrator:

The Fiber Optic Sensing Association ("FOSA") appreciates the opportunity to submit comments to the Transportation Security Administration ("TSA") regarding the Advance Notice of Proposed Rulemaking (ANPRM) on Enhancing Surface Cyber Risk Management; 49 C.F.R. Chapter XII, Docket No. T.S.A.–2022–0001 Federal Register Number: 73527-73538 (November 30, 2022) RIN 1652–AA74

FOSA was founded in 2017 as a non-profit trade association to educate industry, government, and the general public on the benefits of fiber optic sensing technologies that enhance public safety, promote the security of critical facilities and infrastructure and protect the environment. Our members include organizations that manufacture, install, test, evaluate, support, and/or use fiber optic sensing systems and equipment.[ii]

I. Technical Discussion - Distributed Fiber Optic Sensing (DFOS)

A. Overview

Distributed and quasi-distributed fiber optic sensors connect optoelectronic interrogators to an optical fiber or cable, converting the fiber to an array of distributed sensors. The fiber becomes the sensor while the interrogator injects laser energy into the fiber and detects events along the fiber. This technology can be deployed to continuously monitor vehicle movement, foot traffic, digging activity, seismic activity, temperatures, structural integrity, liquid or gas leaks, and many other conditions and activities. It is used worldwide to monitor power stations, telecom networks, railways, roads, bridges, international borders, critical infrastructure, terrestrial or subsea power cables or pipelines, and downhole applications in oil, gas, and enhanced geothermal electricity generation.

Fiber optic sensing is not constrained by line of sight or remote power access. Depending on system configuration, it can be deployed in continuous lengths exceeding 45 km (30 miles) with detection at every point along its path. Competing technologies cannot match the cost per sensing point over great distances. If fiber optic cable has already been deployed fiber within a previously installed cable can be used for sensing.

Fiber optic sensing measures changes in an optical fiber's naturally occurring "backscattering" of light. Measurable change is observed when the fiber encounters vibration, strain, or temperature change. The fiber serves as a sensor over its entire length, delivering real-time information on physical surroundings and security. Furthermore, the data instantaneously pinpoints the precise location of events and conditions occurring at or near the sensor cable.

Several DFOS methods are used:

- **Distributed Acoustic Sensing (DAS)** can monitor the vibration characteristics of assets such as a pipeline or railroad right-of-way and quickly detect unauthorized or unexpected third-party interference or intrusion by monitoring the vicinity of the infrastructure asset. DAS can go as far as to determine the potential cause of the vibrations and, therefore, alert the rail or pipeline operator of the specific nature of the potential threats. DAS can also be used to detect associated events, such as leaks by sensing multiple effects on the fiber.
- **Distributed Temperature Sensing (DTS)** is deployed to monitor the subtle temperature variations on or around a linear asset. From effects due to product escaping a pipeline to subtle changes along a railbed, DTS is suitable to report absolute temperatures that help characterize events, pinpoint areas of concern, and track subtle changes occurring with time – providing alerts and alarms as appropriate.

- **Distributed Strain Sensing (DSS)** is deployed along or on pipelines or rail rights-of-way to monitor changes in the strain that shifts in the soil in the vicinity of the asset might cause. If the strain from these soil shifts grows large enough, it can cause the pipeline or railroad track to shift, buckle, and even rupture. DSS is an ideal tool for use in the prevention of catastrophic events that are known to occur with aging assets.

B. Pipelines

Pipeline monitoring represents one of the most common uses for DFOS. Among these are:

- Detecting unauthorized or unexpected third-party interference near the pipeline;
- Detecting excessive strain being applied to the pipeline due to shifts in the soil caused by subsidence, landslides or other geotechnical reasons;

- Detecting soil erosion and water ingress as means of very early warning and prevention;
- Detecting pipeline leaks, ruptures, or valve operation, whether liquid, gas or a combination of liquid and gas;
- Detecting negative pressure waves traveling inside pipelines; and
- Tracking the instrumentation position and cleaning PIGs (Pipeline Inspection Gauges/Gadgets).

Monitoring these conditions is very important to pipeline operators. Third-party interference, whether intentional or not, and excessive strain can lead to a pipeline leak. These need to be reported to the pipeline operator as soon as possible.

DFOS methods provide significant advantages for pipeline operators, complementing traditional Computational Pipeline Monitoring Leak Detection Systems (CPM LDS) by adding prevention through very early detection. Additionally, DFOS instantaneously pinpoints sudden operating changes at all points along the asset and issues alerts/alarms to hasten responses and mitigate harm.

C. Railroads

For railroads, distributed fiber optic sensing techniques, such as DAS, DSS or DTS, are potent tools for monitoring long, linear assets. These technologies serve the specific requirements of the railroads, such as:

- Detecting trackside activity (work crews, trespassers, cable tampering)
- Tracking the position, direction, speed & length of trains
- Monitoring rolling stock defects (flat/defective wheels and defective bearings)
- Monitoring rail defects (rail breaks, rail buckling or bad welds/joins)
- Detecting Rockfall and landslide events in the vicinity of the track

In each application, distributed fiber optic sensing offers a clear benefit in covering a wide area from a central monitoring point. It can often achieve this by repurposing spare fibers in the existing railroad communication network.

II. Regulatory Discussion

Critical infrastructure, including rail and pipelines, depends on long-haul/telecommunications networks, Industrial Control Systems (ICS), Operation Technology (OT), and Supervisory, Control and Data Acquisition (SCADA) Systems for crucial functions. Increasingly, as digital and physical systems become more integrated, these systems charged with managing critical infrastructure activities also directly connect to the Internet and share sensitive data. This hybrid structure requires that these vital infrastructure components apply enhanced attention to security considerations.

Fiber optic cable commonly provides the backbone of these communications connections. A single fiber strand within a cable carries massive amounts of information. This functional importance makes it an attractive target for attackers intent on intercepting proprietary company and customer information or disrupting service. These outcomes have the potential to create disastrous consequences.

Distributed fiber optic sensing solutions can be used to detect perimeter intrusions. These may include security solutions performing continuous monitoring and analysis of cables, pathways, and points of vulnerability such as fence lines, barriers, roadways, campus perimeters, manholes and equipment cabinets. The technology helps with the timely identification of intrusions that are often precursors to a physical attack or damage that could degrade network performance or availability. Perimeter intrusion detection solutions can be enhanced by incorporating additional detection algorithms. For example, they can be used to monitor barrier fence lines to detect attempts to climb over, tunnel under, or cut through, providing a physical layer of security and immediate alert for protecting personnel, property, and equipment.

In addition to pipelines and rail, other critical infrastructure sectors share the common need to protect their vital information that flows over communication systems, prevent unauthorized access into areas based on public safety, and protect dangerous or high-value assets.

The ANPRM appropriately encourages respondents to provide cost estimates for cybersecurity solutions. As the notice observes, the relevant public standards, including the NIST Framework for Improving Critical Infrastructure Cybersecurity, incorporate guidance on balancing costs with risks.[iii] Incorporating distributed fiber optic sensing within an infrastructure asset's security architecture can be consistent with these considerations.

Distributed fiber optic sensing's principal cost can often be the installation of fiber optic cable along asset rights-of-way. However, this expense can be offset when fiber optic cable is already located or when the new fiber is also being installed to enable communications (e.g. Middle Mile Broadband).

Estimates vary regarding the millions of miles of fiber optic cable in the U.S. and the proximity along extended linear critical infrastructure.[iv] FOSA notes that public policy for broadband strongly encourages a "multi-use" approach, that is, using existing currently deployed fiber to support multiple services.[v]

As the NTIA has noted," many programs across the federal government include broadband as one of many eligible expenses. While these programs may support many of the same activities as broadband programs, their missions include promoting economic growth, expanding healthcare access, improving education, and constructing community housing, facilities, and other public infrastructure."[vi] Consequently, available fiber optic cable may have been installed proximate to infrastructure for various initial reasons. Nevertheless, that presence creates the opportunity for the available cable of commercially deployed fiber to be used economically to enable fiber optic sensing to enhance

security. Consistent with this is the use of fiber optic cable for sensing to detect intrusion and provide security alerts for intrusions.

The ANPRM poses several questions regarding security mandates. These include seeking recommendations on security controls (D.12.); baseline physical security (D.14.); security of third-party service providers (D.13.). FOSA notes that the business case for DFOS deployment by pipelines and railroads typically is made independent of its cyber-security benefits. However, where DFOS technology is added, then cyber-security enhancements can be an added benefit.

III. Conclusion

Our association welcomes the opportunity to work supportively with TSA, railroads, pipeline operators, and other owners of critical infrastructure owners to achieve the policy objectives expressed by this ANPRM. We commend the TSA for the agency's leadership in protecting the nation's critical assets.

Sincerely,

Mark Uncapher

Mark Uncapher,
Executive Director

[i] Federal Register 85, no. 25 (February 6, 2020): 7162.
[ii] For more information regarding the Fiber Optic Sensing Association, see https://www.fiberopticsensing.org/
[iii] National Institute of Standards and Technology, 2018. *Framework for Improving Critical Infrastructure Cybersecurity*. National Institute of Standards and Technology (NIST).
[iv] S&P Global Market Intelligence, Fiber Route Mile Leaderboard, March 2019 https://www.spglobal.com/marketintelligence/en/news-insights/blog/fiber-route-mile-leaderboard (accessed January 30, 2023)
[v] NTIA ACCESS BROADBAND 2021 Report, https://www.ntia.doc.gov/files/ntia/publications/ntia_access_broadband_2021_report.pdf (accessed January 30, 2023)
[vi] National Telecommunications and Information Administration (NTIA) ACCESS BROADBAND 2021 Report December 2021 https://www.ntia.doc.gov/files/ntia/publications/ntia_access_broadband_2021_report.pdf