EXHIBIT A

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

SUNOCO PIPELINE L.P., Plaintiff, v. U.S. DEPARTMENT OF TRANSPORTATION, PIPELINE AND HAZARDOUS MATERIALS SAFETY ADMINISTRATION, PETER BUTTIGIEG, SECRETARY OF THE DEPARTMENT OF TRANSPORTATION, IN HIS OFFICIAL CAPACITY, AND TRISTAN BROWN, ACTING ADMINISTRATOR OF THE PIPELINE AND HAZARDOUS MATERIALS SAFETY ADMINISTRATION, IN HIS OFFICIAL CAPACITY, Defendants.	Civil Action No. 1:21-cv-01760-TSC

BRIEF OF AMICI CURIAE THE AMERICAN FUEL & PETROCHEMICAL MANUFACTURERS, AMERICAN GAS ASSOCIATION, AMERICAN PETROLEUM INSTITUTE, ASSOCIATION OF OIL PIPE LINES, INTERSTATE NATURAL GAS ASSOCIATION OF AMERICA, AND NATIONAL ASSOCIATION OF MANUFACTURERS IN SUPPORT OF PLAINTIFF'S OPPOSITION TO DEFENDANTS' MOTION TO DISMISS

CORPORATE DISCLOSURE STATEMENT

Per Civil Rule 26.1 of the Local Rules of the United States District Court for the District of Columbia, the amici curiae state that none of them has a parent corporation and no publicly held company owns 10% or more of any amici's stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Rules, Statutes, and Orders

Other Authorities

INTEREST OF AMICI CURIAE

Amici Curiae the American Fuel & Petrochemical Manufacturers, American Gas Association, American Petroleum Institute, Association of Oil Pipe Lines, Interstate Natural Gas Association of America, and National Association of Manufacturers (collectively, "the Associations") submit this brief in support of Sunoco Pipeline L.P.'s opposition to the Defendants' motion to dismiss.[1] The Associations' members customarily protect the type of information at issue in this case from public disclosure due to significant threats to disruption of operations and public safety from terrorists and other bad actors seeking to exploit potential vulnerabilities. Their members submit such information to regulators with the reasonable expectation that the Freedom of Information Act's (FOIA) exemptions will prevent disclosure of confidential safety-related information. The Government's decision to disregard the applicable FOIA exemptions to Plaintiff's information presents grave concerns regarding the treatment of similar information that the Associations' members routinely provide to regulators. The Associations submit this brief to highlight their concerns about the public safety and confidentiality interests at stake.

The Associations represent the spectrum of the country's energy infrastructure and manufacturers, which are some of the nation's largest energy consumers.

American Fuel & Petrochemical Manufacturers (AFPM): AFPM is a national trade association representing most U.S. refining and petrochemical manufacturing capacity and the midstream companies that move feedstocks and products where they need to go. These companies provide jobs, directly and indirectly, to more than three million Americans, contribute to our economic and national security, and enable the production of thousands of vital products used by families and businesses throughout the nation.

American Gas Association (AGA): AGA represents more than 200 local energy companies that deliver natural gas throughout the United States. There are more than 76 million

[1] No counsel for a party authored this brief in whole or in part. No party, no counsel for a party, and no person other than Amici, their members, and their counsel made a monetary contribution intended to fund the preparation or submission of this brief.

residential, commercial, and industrial natural gas customers in the U.S., of which 95 percent—more than 72 million customers—receive their gas from AGA members.

American Petroleum Institute (API): API represents all segments of America's natural gas and oil industry, which supports more than 11 million U.S. jobs and is backed by a growing grassroots movement of millions of Americans. API's nearly 600 members produce, process, and distribute most of the nation's energy, and participate in API Energy Excellence, which is accelerating environmental and safety progress by fostering new technologies and transparent reporting.

Association of Oil Pipe Lines (AOPL): AOPL promotes responsible policies, safety excellence, and public support for liquids pipelines. AOPL represents pipelines transporting 97 percent of all hazardous liquids barrel miles reported to the Federal Energy Regulatory Commission. Its diverse membership includes large and small pipelines carrying crude oil, refined petroleum production, natural gas liquids, and other liquids.

Interstate Natural Gas Association of America (INGAA): INGAA is a trade organization that advocates regulatory and legislative positions of importance to the natural gas pipeline industry in North America. INGAA is composed of 26 members, representing the vast majority of the interstate natural gas transmission pipeline companies in the U.S. and Canada. INGAA members operate almost 200,000 miles of pipeline.

National Association of Manufacturers (NAM): NAM works for the success of the more than 12.8 million men and women who make things in America. Representing 14,000 member companies—from small businesses to global leaders—in every industrial sector, NAM is the nation's most effective resource and most influential advocate for these values and for manufacturers across the country.

The Associations oppose the Government's motion to dismiss Sunoco's complaint because their members closely guard confidential commercial and security information, like the risk-consequence modeling data at issue here, to protect their own commercial interests and the public. The Government's position in this case is concerning because it opens the door to disclosure of

information that presents serious risks if placed in the wrong hands. Not only does this threaten the right of regulated industries to appropriately protect the confidentiality of private information, but it threatens the safety of our Nation's energy infrastructure.

SUMMARY OF ARGUMENT

Energy infrastructure is a critical part of our national economy and the everyday lives of all Americans. *See, e.g.*, ENERGY SECTOR-SPECIFIC PLAN 1 (2015), https://bit.ly/3aDXuKA; *see also* Compl. ¶ 54. In part because of the critical nature of energy infrastructure, the Government requires the Associations' members to provide risk-modeling information to help protect against and plan for the potential impacts of a major physical or cyber attack.

The Associations' members provide this information to regulators on the expectation that it will be kept confidential. And historically, it has been kept confidential.

But now the Government seeks to release this kind of information to the public. Making this information public would be contrary to FOIA Exemptions 4 and 7(F). Through FOIA Exemption 4, "Congress has instructed that the disclosure requirements of the Freedom of Information Act do 'not apply' to 'confidential' private-sector 'commercial or financial information' in the government's possession." *Food Mktg. Inst. v. Argus Leader Media*, 139 S. Ct. 2356, 2360 (2019). And "Exemption 7(F) evince[s] congressional understanding of the many potential threats posed by the release of sensitive agency information" that "could be misused for nefarious ends." *Public Emps. for Envtl. Responsibility v. U.S. Section, Int'l Boundary & Water Comm'n, U.S.-Mexico*, 740 F.3d 195, 206 (D.C. Cir. 2014) (hereinafter "*PEER*"). *See also Standing Rock Sioux Tribe v. U.S. Army Corps of Engineers*, 249 F. Supp. 3d 516, 522-23 (D.D.C. 2017) (protecting spill-model reports in reverse FOIA claim brought by pipeline because "in Exemption 7(F) cases involving documents relating to critical infrastructure, it is not difficult to show that disclosure may endanger the life or physical safety of any individual" (internal quotation marks and citation omitted)). Releasing this information publicly would be damaging. Risk-modeling data from private corporations does not provide insight into "what [the] government is up to," which is "the only relevant public interest in the FOIA balancing analysis." *U.S. Dep't of*

Defense v. Fed. Labor Relations Auth., 510 U.S. 487, 497 (1994) (internal quotation marks and citation omitted). Instead, releasing risk-modeling data could provide more information to people with ill intentions, to the detriment of everyone.

ARGUMENT

I. Protecting Risk-Consequence Modeling Data from Public Disclosure Is Crucial to Safety, Security, and Commercial Interests.

In 2013, President Obama identified 16 critical infrastructure sectors that provide "the essential services that underpin American society." PRESIDENTIAL POLICY DIRECTIVE — CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE, PRESIDENTIAL POLICY DIRECTIVE/PPD-21 (Feb. 12, 2013), https://bit.ly/3C4JfKY. Those sectors include chemical, critical manufacturing, energy, transportation, and water and wastewater systems. *Id.* The President recognized that "secure, functioning, and resilient critical infrastructure requires the efficient exchange of information, including intelligence, between all levels of governments and critical infrastructure owners and operators." *Id.* To ensure the safety of these sectors, he noted that the federal government must "facilitate the timely exchange of threat and vulnerability information as well as information that allows for the development of a situational awareness capability during incidents." *Id.* "Greater information sharing within the government and with the private sector can and must be done while respecting privacy and civil liberties." *Id.*

Both President Trump and President Biden have built on this initiative. For the entities classified as "critical infrastructure at greatest risk" by President Obama, President Trump directed federal agencies to "identify authorities and capabilities that agencies could employ to support [their] cybersecurity efforts" and engaging with these entities to "support their cybersecurity risk management efforts." Exec. Order No. 13,800 § 2(a), (b)(i), 82 Fed. Reg. 22,391, 22,393 (May 11, 2017); *see also* Exec. Order No. 13,636 § 9, 78 Fed. Reg. 11,739, 11,742 (Feb. 12, 2013). President Biden required federal agencies to "develop and issue cybersecurity performance goals for critical infrastructure to further a common understanding of the baseline security practices" they "should follow to protect national and economic security, as well as public health and safety." NATIONAL

SECURITY MEMORANDUM ON IMPROVING CYBERSECURITY FOR CRITICAL INFRASTRUCTURE CONTROL SYSTEMS, § 4(a) (July 28, 2021), https://bit.ly/3pov5kr.

These principles of protecting infrastructure from physical and cybersecurity threats remain critically important today. Roughly two-thirds of U.S. energy demand is transported by pipeline, making pipelines a significant target for terrorists and other bad actors who would want to disrupt U.S. energy systems. *See, e.g.*, Joseph R. Dancy & Victoria A. Dancy, *Terrorism and Oil & Gas Pipeline Infrastructure: Vulnerability and Potential Liability for Cybersecurity Attacks*, 2 OIL & GAS, NAT. RESOURCES & ENERGY J. 579, 580 (2017). And the more than 2.7 million miles of pipelines literally fueling the economy operate under the threat of "malicious physical attack." U.S. GOV'T ACCOUNTABILITY OFF., GAO-19-426, CRITICAL INFRASTRUCTURE PROTECTION: KEY PIPELINE SECURITY DOCUMENTS NEED TO REFLECT CURRENT OPERATING ENVIRONMENT 1 (2019), https://bit.ly/3jqV9HO ("GAO REPORT"); *Pipelines: Securing the Veins of the American Economy Before the Subcomm. on Transportation Security*, 114th Cong. (2016) (statement of Paul Parfomak, Specialist in Energy and Infrastructure at the Congressional Research Service) ("Parfomak Statement"), https://bit.ly/3b1dBlO.

The threat of attack against critical energy infrastructure is clear, present, and ongoing. For example, in 2021, a Swedish lecturer and author published HOW TO BLOW UP A PIPELINE: LEARNING TO FIGHT IN A WORLD ON FIRE. When discussing the book, the author advocated for "destroying machines [and] property" associated with fossil fuel infrastructure as part of a campaign of "intelligent sabotage." David Remnick, Podcast: Should The Climate Movement Embrace Sabotage?, THE NEW YORKER (Sept. 24, 2021), https://bit.ly/3B7OLeh. The author went on to explain that "property can be destroyed in all manner of ways or it can be neutralized . . . in a more spectacular fashion as in potentially blowing up a pipeline that is under construction." *Id.*

Just this week, protestors in Michigan trespassed and tampered with a pipeline, forcing the company to shut it down for several hours. Nia Williams, *Enbridge Briefly Shut Line 5 After Protesters Tampered with Pipeline*, REUTERS (Oct. 20, 2021), https://reut.rs/3G5IROF. In April 2021, hackers infiltrated Colonial Pipeline Company's computer networks. William Turton &

Kartikay Mehrotra, *Hackers Breached Colonial Pipeline Using Compromised Password*, BLOOMBERG (Jun. 4, 2021), https://bloom.bg/3aEczMc. In 2011, an individual planted a bomb, which did not detonate, along a natural gas pipeline in Oklahoma. *See* Parfomak Statement. In 2007, the U.S. Department of Justice arrested members of a terrorist group planning to attack jet-fuel pipelines and storage tanks at the John F. Kennedy International Airport. *Id.* And in 2005, a U.S. citizen sought to conspire with Al Qaeda to attack a major natural gas pipeline in the eastern region of the United States. *Id*.

The direct and indirect consequences of terrorist actions against pipelines are severe and affect nearly all aspects of the economy. The direct effects include physical damage to infrastructure. For example, a 2014 cyber-attack on a German steel mill led to the loss of control of a blast furnace, causing significant damage to the plant. DELOITTE CENTER FOR ENERGY SOLUTIONS, *Refining at Risk: Securing Downstream Assets from Cybersecurity Threats* (2017) 3, https://bit.ly/3BOTZgh. The indirect effects could include "commodity price increases," "widespread energy shortages," and effects on "other domestic critical infrastructure and industries that are dependent on pipeline system commodities." GAO REPORT 2.

The Colonial Pipeline hack mentioned above is illustrative. After the hackers issued a ransom note, Colonial Pipeline Company shut down the pipeline as a prophylactic measure, and the loss of this critical infrastructure caused long lines at gas stations and higher fuel prices. Turton & Mehrotra, *supra*. Further, fuel and petrochemical manufacturers depend on pipelines to deliver an uninterrupted, affordable supply of crude oil and natural gas as feedstocks for the transportation fuels and petrochemicals they manufacture. Indeed, manufacturers use one-third of all energy consumed in the United States and can face significant disruption and cost overruns when infrastructure is destabilized.[2]

Given the critical nature of these resources and the potential for human and economic harm, hazard and risk analyses are part of pipeline operators' integrity management plans, *see* Compl.

[2] National Association of Manufacturers, Policy Issues, Energy, https://bit.ly/3FQTswQ (Oct. 22, 2021).

¶ 20, that is, programs to inspect and maintain their pipeline systems. Operators also use these analyses to cooperate with federal, state, and local governments for emergency preparedness. *Id.*

The Government claims that disclosure does not implicate any security concern because the documents at issue lack the *exact* geographic locations of the most vulnerable points in the pipeline. Mem., Dkt. No. 12-1, at 11-12. However, Sunoco's risk-assessment and consequence-modeling data could provide a roadmap for bad actors intending to maximize damage to public safety and pipeline operations. Sunoco's risk assessment and consequence modeling includes information about areas along the pipeline that would be most affected by a potential pipeline rupture, as well as distances where the impact from a catastrophic pipeline rupture would be the greatest, i.e., which local communities would be most affected. Compl. ¶¶ 20, 53. This puts communities, the pipeline, and all energy infrastructure at greater risk of harm. In short, bad actors can use risk-consequence analyses to assess, select, and target infrastructure that they believe is most vulnerable to, or could cause the most harm from, a physical or cyber-attack.

II. The Government May Not Release These Confidential Documents

Sunoco's risk-consequence modeling documents are protected from disclosure under FOIA by both Exemption 4 and 7(F). Defendants' decision to disclose such documents would be contrary to law.

A. FOIA Exemption 4 protects commercial information, like risk-consequence modeling data, from public disclosure.

FOIA's Exemption 4 broadly applies to commercial information that companies customarily shield from public disclosure. Exemption 4 shields from disclosure "trade secrets and commercial or financial information obtained from a person [that is] privileged and confidential." 5 U.S.C. § 552(b)(4). "[I]nformation communicated to another remains confidential whenever it is customarily kept private, or at least closely held, by the person imparting it." *Argus Leader Media*, 139 S. Ct. at 2363 (collecting authorities). And whether information is commercial boils down to whether the proponent has a "business interest" in that information. *Renewable Fuels*

Ass'n v. Envtl. Protection Agency, 519 F. Supp. 3d 1, 8 (D.D.C. 2021) (internal quotation marks and citation omitted).

Risk-consequence modeling data is both confidential and commercial. The Associations' members customarily keep risk-consequence modeling and similar data private. They closely hold information like risk-consequence modeling data because disclosure could threaten operational integrity if placed in the wrong hands. Infrastructure operators therefore have strong commercial and public interests in protecting that information from disclosure. Indeed, the Department of Homeland Security, the federal agency primarily charged "to secure the nation from the many threats we face,"[3] has recognized that risk assessments are "not only a common business practice, but also a mission of individual owners and operators to ensure the security and protection of their own assets. For that reason, as part of everyday operation, they develop and apply facility and system risk assessment methodologies." Cybersecurity & Infrastructure Security Agency, Critical Infrastructure Sectors, ENERGY SECTOR-SPECIFIC PLAN at 13.

Regulators such as the Pipeline and Hazardous Materials Safety Administration (PHMSA) play an important role in overseeing the safety and security of these assets but doing so requires that operators cooperate and coordinate with them under regulatory requirements and best practices. Publicizing risk assessment information undermines those efforts by exposing the same information needed to maintain security. The Associations' concerns about the Government's position in this case are heightened because of the massive amounts of information regarding critical infrastructure they provide to PHMSA and other agencies, which may include sensitive information.[4] For example, PHMSA alone requires risk modeling for most of the millions of miles

---

[3] Dep't of Homeland Sec., About DHS, https://bit.ly/3AZx9kU (last visited Oct. 22, 2021).

[4] To illustrate, operators prepare confidential risk and consequence information, which informs the following PHMSA regulatory requirements, among others: operator emergency preparedness plans and activities, 49 C.F.R. §§ 195.403, 192.615; public awareness programs, *id*. §§ 195.440, 192.616; liquid operators' facility response plan for worst case discharge and spill modeling, *id.* § 194.107; leak detection evaluations, *id*. §§ 195.444, 195.452(i)(3); integrity management threat identification and risk modeling, *id*. §§ 195.452(g); 192.917, 192.1007; preventive and mitigative measures risk evaluation, *id*. §§ 195.452(i)(2), 192.935, 192.1007; and

of oil and gas pipelines in the country. Until now, PHMSA has treated information relating to the areas of risk identified in the modeling as confidential and Amici's members have relied on that confidentiality to help protect their infrastructure.

Companies also protect information like risk-consequence modeling data because it is important to their competitive interests. "A company has a clear commercial interest in its basic business operations and techniques." *Public Citizen v. U.S. Dep't of Health & Human Servs.*, 66 F. Supp. 3d 196, 207 (D.D.C. 2014) (internal quotation marks and citation omitted). Risk-consequence modeling forms a basic part of commercial operations for pipeline operators. For example, it provides information necessary to internal operations, including in the development of risk-preparedness procedures, maintenance protocols, and related analyses. Risk-consequence modeling also is required by federal regulation, making it integral to a pipelines' ability to lawfully operate. Although this type of information is disclosed to the government to further public safety and security, it is not disclosed to competitors who could use the information to gain competitive advantage (e.g., through anticipating maintenance operations or operational cost sensitivities).[5]

Given these strong interests in both security and commercial sensitivity, Amici's members customarily seek and maintain confidential status over risk-consequence modeling data and similar information.

B. FOIA Exemption 7(F) also protects risk consequence modeling data from disclosure to protect against threats to public safety.

Exemption 7(F) protects from disclosure "records or information compiled for law enforcement purposes, but only to the extent that the product of such law enforcement records or information . . . could reasonably be expected to endanger the life or physical safety of any

---

emergency flow restricting device, automatic shut-off valves, and/or remote-control valves analyses, *id.* § 195.452(i)(4), 192.935(c).

[5] As Sunoco explains in its response to Defendants' motion to dismiss, Exemption 4 is bolstered by the Trade Secrets Act. *See* Pl.'s Resp. to Defs.' Mot. To Dismiss, Dkt. No. 13, at 12-14 (noting that the Trade Secrets Act is coextensive with Exemption 4, precluding government disclosure of information that falls within the Exemption and subjecting disclosure to review under the APA).

individual." 5 U.S.C. § 552(b)(7)(F). Courts have considered an agency to perform a law enforcement function where it seeks to "enhance . . . protection of human life and property" because "[t]hat duty necessarily encompasses security and prevention of criminal or terrorist attacks." *PEER*, 740 F.3d at 204 (internal quotation marks and citation omitted). Therefore, under Exemption 7(F) "records and information compiled for law enforcement purposes" includes "proactive steps designed to prevent criminal activity and to maintain security." *Elec. Privacy Info. Ctr. v. U.S. Dep't of Homeland Sec.*, 777 F.3d 518, 522 (D.C. Cir. 2015) (hereinafter "*EPIC*") (internal quotation marks and citation omitted).

In that vein, Exemption 7(F) includes information that agencies collect from regulated entities to protect important infrastructure and the public from critical emergencies. *EPIC*, 777 F.3d at 523. In fact, "the government . . . will ordinarily be able to satisfy Exemption 7(F) for documents relating to critical infrastructure, such as emergency plans." *Id.* (cleaned up; citation omitted). For example, in *PEER* the D.C. Circuit shielded emergency action plans and inundation maps for two dams from disclosure under FOIA. 740 F.3d at 203-04. And in *EPIC* the D.C. Circuit held a company's protocol for shutting down wireless networks during critical emergencies was exempt from disclosure under FOIA. 777 F.3d at 528.

The type of risk-consequence data at issue here can similarly endanger life and physical safety if released publicly. As described above, when placed in the wrong hands, it can be used to identify vulnerabilities that can be exploited by bad actors. The Government repeatedly has identified and warned of these types of threats. *See, e.g.*, AMERICAN PETROLEUM INSTITUTE, UTILIZING INTELLIGENCE TO SECURE PEOPLE, OPERATIONS AND ASSETS: AN INTRODUCTION TO USES AND SOURCES 3-4 (Aug. 2015), https://bit.ly/3FKIGbv. And, as noted above, pipelines are a known target. In cases like this, disclosure "could reasonably be expected to endanger the life or physical safety of any individual." 5 U.S.C. § 552(b)(7)(F).

C. Disclosing this type of information is contrary to FOIA's balance between open government and protection of private sector interests.

FOIA seeks to serve the public interest in monitoring what the *government* is doing. *Fed. Labor Relations Auth.*, 510 U.S. at 497. Recognizing that government activity sometimes includes private information, Congress "sought a 'workable balance' between disclosure and other governmental interests—interests that may include providing private parties with sufficient assurances about the treatment of their proprietary information so they will cooperate in federal programs and supply the government with information vital to its work." *Argus Leader Media*, 139 S. Ct. at 2366 (citation omitted) (protecting confidential commercial information from disclosure to South Dakota newspaper). But ensuring the public has access to "what [the] government is up to," is "the only relevant public interest in the FOIA balancing analysis." *Fed. Labor Relations Auth.,* 510 U.S. at 497 (internal quotation marks and citation omitted). To that end, Exemptions 4 and 7(F) help ensure that inquiries into what the government is doing do not jeopardize the confidentiality of private commercial and security information that private actors must share with the government. And companies operating critical infrastructure rely on the confidential status of this information when disclosing risk analyses to the government. Disclosing it after the fact threatens their ability to plan and evaluate additional threats to their business interests and operations posed by the public disclosure of information. Simply put, revealing Sunoco's information sheds no light on "what the government is up to" and jeopardizes private interests. That should be the end of the inquiry.

CONCLUSION

For these reasons, the Court should deny Defendants' motion to dismiss.

Dated: October 22, 2021

Respectfully submitted,

/s/ Steven P. Lehotsky
Steven P. Lehotsky (DC Bar No. 992725)
Michael B. Schon (DC Bar No. 989893)*
Gabriela Gonzalez-Araiza (DC Bar No. 1631972)*
LEHOTSKY KELLER LLP
200 Massachusetts Avenue NW
Washington, DC 20001
steve@lehotskykeller.com
T: (512) 693-8350

* *Application for admission to the D.D.C. bar pending*

CERTIFICATE OF SERVICE

I hereby certify that on October 22, 2021, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notice of electronic filing to all counsel of record who have consented to electronic notification.

/s/ Steven P. Lehotsky
Steven P. Lehotsky

CERTIFICATE OF COMPLIANCE

Pursuant to LCvR7(o), I certify that this brief is 12 pages and complies with LCvR5.4 and Federal Rule of Appellate Procedure 29(a)(4).

/s/ Steven P. Lehotsky
Steven P. Lehotsky