IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

SUNOCO PIPELINE, L.P., *Plaintiff*, v. U.S. DEPARTMENT OF TRANSPORTATION, *et al.*, *Defendants*.	Case No. 1:21-cv-01760-TSC

PROPOSED BRIEF OF THE CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA AS *AMICUS CURIAE* IN SUPPORT OF PLAINTIFF

Paul V. Lettow (D.C. Bar No. 502440)
Andrew R. Varcoe (D.C. Bar No. 473834)
U.S. CHAMBER LITIGATION CENTER
1615 H Street, NW
Washington, DC 20062
(202) 463-5337

John P. Elwood (D.C. Bar No. 452726)
Janine M. Lopez* (D.C. Bar No. 1685754)
ARNOLD & PORTER KAYE SCHOLER LLP
601 Massachusetts Avenue, NW
Washington, DC 20001
(202) 942-5000
John.Elwood@arnoldporter.com

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

Counsel for Amicus Curiae

CORPORATE DISCLOSURE STATEMENT

The Chamber of Commerce of the United States of America certifies that it is a non-profit trade association. The Chamber has no parent company, and no publicly held company has 10% or greater ownership in the Chamber.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Rules and Regulations

Other Authorities

INTEREST OF *AMICUS CURIAE*[1]

The Chamber of Commerce of the United States of America ("Chamber") is the world's largest business federation. The Chamber represents approximately 300,000 direct members and indirectly represents more than three million businesses and professional organizations of every size, in every sector, and from every geographic region of the country. An important function of the Chamber is to represent the interests of its members in matters before the courts, Congress, and the Executive Branch. To that end, the Chamber regularly files *amicus curiae* briefs in cases, like this one, that raise issues of concern to the nation's business community.

The Chamber's members frequently submit sensitive information to the federal government—whether voluntarily, as a condition of obtaining a government benefit, or under mandatory reporting provisions. Whether such information is subject to public disclosure under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, is of great importance to the Chamber and its members. Accordingly, the Chamber has a substantial interest in the proper interpretation of FOIA's exemptions, including the two exemptions at issue in this case.

The Chamber has a similarly weighty interest in ensuring that private parties can obtain judicial review of an agency's decision to disclose their information. Private businesses that are *required* to report information to government agencies would face significant risks if agencies could arbitrarily disclose that information—including the risk of exploitation by competitors or bad actors. Private businesses that *voluntarily* report information to the government (or submit information as a condition of participating in a government program) would face similar concerns, and would be unable to make informed judgments about whether to continue sharing sensitive

[1] *Amicus curiae* states that no counsel for any party authored this brief in whole or in part and no entity or person, aside from *amicus curiae*, its members, or its counsel, made any monetary contribution intended to fund the preparation or submission of this brief.

materials with the government. That, in turn, may affect the efficacy of government programs that depend on strong cooperation between government and private parties.

INTRODUCTION

The government requires information from the governed in order to function. A substantial amount of that information is confidential and highly sensitive, as this case illustrates. During an inspection of one of Sunoco's pipeline systems, the company submitted modeling information predicting the areas that would be "most impacted" by a pipeline rupture and identifying the worst-case scenarios for those areas. Compl. ¶¶ 17-20. As Sunoco has explained (Opp'n 18-19), third parties intent on harming the United States could use this information to cause catastrophic damage to the pipeline, to surrounding communities, and potentially to national security and the economy. Yet the government surprisingly claims not only that it may release this information to the public, but also that pipeline operators like Sunoco have *no* legal recourse to prevent its disclosure.

That is not the law. Congress recognized in FOIA that not all information submitted to the government can or should be disclosed; "legitimate governmental and private interests could be harmed by release of certain types of information," and FOIA's exemptions are meant to safeguard those interests. *FBI v. Abramson*, 456 U.S. 615, 621 (1982). Accordingly, the Supreme Court and the D.C. Circuit have long held that a private party seeking to prevent disclosure can obtain review of an agency's disclosure decision under the Administrative Procedure Act ("APA"), which requires courts to set aside decisions that are "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(2)(A). This check on agencies' discretion serves important government interests: Regulated entities are substantially more likely to provide the information the government needs if they are assured that their private, sensitive information will not be publicly disclosed—and that they can obtain timely and effective judicial review before an agency illegally discloses such information.

Here, Sunoco correctly argues that the decision of the Pipeline and Hazardous Materials Safety Administration ("PHMSA") to release its modeling information was arbitrary, capricious, and not in accordance with law. The agency failed to rationally explain why the information was not protected by either Exemption 7(F) or Exemption 4. In applying Exemption 7(F), the agency entirely failed to consider the possibility that terrorists, criminals, or other hostile actors could usurp the information to maximize the impact of a pipeline attack. And in applying Exemption 4, the agency mistakenly believed that safety-related information cannot be "commercial" in nature—a position directly at odds with D.C. Circuit precedent. The Court should therefore deny the government's motion to dismiss and allow Sunoco to proceed with its APA claims.

A contrary ruling would have unfortunate consequences not just for national security and all sectors of the national economy; it would also harm the government's own interests as regulator and as partner with private economic actors. Each year, the government requires or requests an extraordinary variety of disclosures from companies in industries as diverse as nuclear waste disposal,[2] banking,[3] real estate development,[4] manufacturing,[5] and agriculture,[6] just to name a few. The information at issue often involves matters of great importance, including public health

[2] *Utah v. DOI*, 256 F.3d 967, 970 (10th Cir. 2001) (addressing information related to utility companies' storage of nuclear waste on tribal land).
[3] *Inner City Press/Cmty. on the Move v. Bd. of Governors of the Fed. Reserve Sys.*, 463 F.3d 239, 242 (2d Cir. 2006) (addressing information in bank merger application submitted to Federal Reserve Board).
[4] *Nadler v. FDIC*, 92 F.3d 93, 94-95 (2d Cir. 1996) (addressing commercial terms of a real estate development agreement signed by a failed bank for which the Federal Deposit Insurance Corporation was appointed as receiver).
[5] *United Techs. Corp. ex rel. Pratt & Whitney v. FAA*, 102 F.3d 688, 689 (2d Cir. 1996) (addressing airplane-engine designs and product specifications submitted to Federal Aviation Administration for approval).
[6] *Lion Raisins, Inc. v. USDA*, 354 F.3d 1072, 1076 (9th Cir. 2004) (addressing reports of inspections at raisin packing facilities), *overruled on other grounds by Animal Legal Def. Fund v. USDA*, 836 F.3d 987 (9th Cir. 2016).

and safety.[7] As this case reveals, however, companies supplying confidential, sensitive information cannot safely presume that the government will take the steps necessary to protect their information from falling into the wrong hands. Where companies have a choice as to whether to share information with the government, they will be far less likely to do so if they have no meaningful recourse when the government illegally decides to disclose their information. And companies that are required to share information with the government will be left in an untenable position, unable to protect their legitimate interests.

ARGUMENT

I. Sunoco Has Stated a Cognizable Reverse-FOIA Claim Under Well-Settled Precedent

The government first contends that Sunoco has not stated a cognizable claim because it has not alleged that disclosure of the requested information would be "contrary to any law." Mot. 7. There are two principal problems with this argument. First, Sunoco *has* adequately alleged that the disclosure of its confidential information would be unlawful. The D.C. Circuit has long held that the scope of the Trade Secrets Act, 18 U.S.C. § 905, "is at least co-extensive" with the scope of Exemption 4. *CNA Fin. Corp. v. Donovan*, 830 F.2d 1132, 1151 (D.C. Cir. 1987). Accordingly, the Act generally prohibits agencies from releasing any information that falls within Exemption 4's scope. *Id.* at 1151-52; *accord Canadian Com. Corp. v. Dep't of Air Force*, 514 F.3d 37, 39 (D.C. Cir. 2008); Dep't of Justice, *Guide to the Freedom of Information Act: Exemption 4* at 18-19 (Oct. 9, 2019) ("[T]he D.C. Circuit has held that if information falls within the scope of Exemption 4, it also falls within the scope of the Trade Secrets Act."). Because Sunoco has

[7] *See, e.g.*, *Pub. Citizen Health Rsch. Grp. v. FDA*, 704 F.2d 1280, 1282-84 (D.C. Cir. 1983) (affected parties were manufacturers of vision-correcting intraocular lenses); *Ctr. for Auto Safety v. NHTSA*, 244 F.3d 144, 145-47 (D.C. Cir. 2001) (involving "information on [automobile] airbag systems").

plausibly alleged that its sensitive pipeline data is protected by Exemption 4, the disclosure of that information would be contrary to law. *See* Opp'n 12-14, 24-29; *see also id.* at 14-17 (explaining that Department of Transportation regulations also bar disclosure of information protected by a FOIA exemption).

Second, the government's position fundamentally misunderstands the Supreme Court's decision in *Chrysler Corp. v. Brown*, 441 U.S. 281 (1979). There, the Supreme Court held that *FOIA itself* does not provide a cause of action to enjoin an agency's disclosure of information. But the Court then made clear that "review of [the agency's] decision" to disclose a private party's data "*is* available under the APA." *Id.* at 317 (emphasis added). The APA prohibits not only decisions that are "not in accordance with law," but also those that are "arbitrary, capricious, [or] an abuse of discretion." 5 U.S.C. § 706(2)(A); *see also CNA Fin. Corp.*, 830 F.2d at 1153-54. A court must therefore set aside a decision to release records under FOIA unless the agency "examine[d] the relevant data and articulate[d] a satisfactory explanation for its action[,] including a 'rational connection between the facts found and the choice made.'" *Motor Vehicles Mfrs. Ass'n of United States, Inc. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983).

Courts have long applied these familiar principles in reverse-FOIA disputes. The D.C. Circuit, for example, has held that it is an APA violation for an agency to fail to explain why it departed from its general nondisclosure policy. *See Qwest Commc'ns Int'l, Inc. v. FCC*, 229 F.3d 1172, 1183 (D.C. Cir. 2000) (requiring the agency to "consider plausible alternatives and discount them" before invoking exception to nondisclosure policy). The court has also held it to be a violation where the agency failed to provide a reasoned basis for disagreeing with a company's contention that disclosing technical information could reveal information about proprietary manufacturing processes to competitors. *See United Techs. Corp. v. U.S. Dep't of Def.*, 601 F.3d

557, 565-66 (D.C. Cir. 2010) (holding that agency acted arbitrarily by providing only a "naked conclusion" as to the possibility of competitive harm). It has held it to be an APA violation where the agency's reasoning depended on factual assertions that the agency could not support. *See Canadian Com. Corp.*, 514 F.3d at 40 (concluding that agency "provided no empirical support" for its assertions that the information at issue had historically been disclosed); *McDonnell Douglas Corp. v. U.S. Dep't of the Air Force*, 375 F.3d 1182, 1190 & n.4 (D.C. Cir. 2004) (holding agency decision was arbitrary and capricious where the agency relied on a "declaration of fact that is 'capable of exact proof' but [was] unsupported by any evidence"). And it has held it to be a violation where the agency simply acted irrationally by relying solely on an out-of-date regulation to justify disclosure. *See Data-Prompt, Inc. v. Cisneros*, No. 94-5133, 1995 WL 225725, at *2 (D.C. Cir. Apr. 5, 1995).

The government offers no reason for disregarding this precedent and *requiring* a reverse-FOIA plaintiff to identify some other law that prohibits disclosure. That position would upset Congress's effort to "provid[e] a workable formula which encompasses, balances, and protects *all* interests," including the interests of private parties that submit information to the government. S. Rep. No. 89-813, at 38 (1965) (emphasis added); *see also Critical Mass Energy Project v. NRC*, 975 F.2d 871, 879 (D.C. Cir. 1992) (en banc) (recognizing "the provider's interest in preventing [the] unauthorized release" of its confidential information). Agencies would be able to avoid accountability for even the most egregious misapplication of FOIA's exemptions—a result that Congress could not have intended.

II. The Agency's Decision to Disclose Sunoco's Modeling Information Was Arbitrary, Capricious, and Not in Accordance with Law

The Court should set aside PHMSA's decision to disclose Sunoco's modeling information, as the agency failed to provide a reasoned explanation for concluding that neither Exemption 4 nor

Exemption 7(F) applied in this case. The Supreme Court has held that an agency decision is ordinarily arbitrary and capricious if the agency has "failed to consider an important aspect of the problem." *State Farm*, 463 U.S. at 43. That is precisely the case here.

A. The Agency Failed to Provide a Reasoned Explanation for Concluding that Disclosure Would Not Endanger the Safety of Individuals

Exemption 7(F) protects law enforcement information that "could reasonably be expected to endanger the life or physical safety of any individual." 5 U.S.C. § 552(b)(7)(F). The D.C. Circuit has expressly addressed this exemption's applicability to critical infrastructure records like the ones at issue here. *See Pub. Emps. for Env't. Resp. v. U.S. Section, Int'l Boundary and Water Comm'n, U.S.-Mex.*, 740 F.3d 195 (D.C. Cir. 2014) ("*PEER*"). That case involved a set of maps "displaying the downstream areas and populations that would be affected" if two dams in the Rio Grande "were to break." *Id.* at 199. The requester believed that the public should be informed of potential "hazards" associated with the dams, but the court held the agency could properly withhold the maps. *Id.* It was "common sense," the court explained, that disclosure could endanger life or public safety; "[t]errorists or criminals could use th[e maps] to determine whether attacking a dam would be worthwhile, which dam would provide the most attractive target, and what the likely effect of a dam break would be." *Id.* at 206. Discussing that decision, the D.C. Circuit has observed that Exemption 7(F) "is broadly stated" and that the exemption "will *ordinarily* be . . . satisf[ied]" by "documents relating to critical infrastructure." *EPIC v. U.S. Dep't of Homeland Sec.*, 777 F.3d 518, 523 (D.C. Cir. 2015) (emphasis added).

PEER's reasoning is equally applicable here. As Sunoco noted, oil and gas pipelines are already "vulnerable to physical attacks" and "continue to be targeted by terrorists and other malicious groups globally." Compl. Ex. M at 9 (quoting U.S. Gov't Accountability Off., *Critical Infrastructure Protection Actions Needed to Address Significant Weaknesses in TSA's Pipeline*

Security Program Management 10-11 (2018)). The May 2021 cyberattack on Colonial Pipeline has underscored both the very real risk of malicious attacks and their potentially immense consequences for public safety and security. *See* Remarks of Acting PHMSA Administrator Tristan Brown at API's Midstream Committee Meeting (May 26, 2021), https://bit.ly/3vxb2kN (explaining that the Colonial incident caused a shutdown of the system that "provides nearly half of the fuel consumed on the East Coast," and advocating for investment in infrastructure "to ensure greater resiliency across the board—including from cyber-attacks"). Sunoco further explained that "[a] hostile actor could use the redacted [modeling] information as a roadmap to determine where or how an attack would cause the greatest harm." Compl. Ex. R at 2. Indeed, the modeling information could inform a future attack on the control technologies that are essential for the pipeline's safe operations. Nonetheless, the agency's final determination summarily concluded that releasing the pipeline information would not endanger public safety. Compl. Ex. T at 8. That analysis "entirely failed to consider" critical aspects of the problem, *State Farm*, 463 U.S. at 43—namely, whether releasing the information would encourage a pipeline attack or potentially increase the damage associated with any attack.

The government now contends that the redacted information does not pose a danger to public safety because it "does not identify any particular areas of weakness or points of vulnerability." Mot. 11 (citing Compl. Ex. T at 6). But the agency has provided no reasoned basis for concluding that only specific information about vulnerable points along the pipeline could reasonably be expected to endanger public safety. *Cf. PEER*, 740 F.3d at 206 (explaining that "[t]errorists or criminals could use [inundation maps] to determine whether attacking a dam would be worthwhile . . . and what the likely effect of a dam break would be"). And that conclusion contradicts PHMSA's own policies protecting worst case discharge information in oil spill

response plans from disclosure. In a 2014 policy, the agency recognized that data inputs used to calculate a pipeline's worst case discharge "could help an outsider gain 'insider information'" about the pipeline infrastructure, which the outsider could then use "to increase the effectiveness of a cyber-attack or physical attack." Compl. Ex. A at 6; *see also id.* (stating that PHMSA would protect information that is "part of the process by which the owner or operator determines the worst case discharge"). The information at issue here—*e.g.*, the maximum predicted spill extent—is similar to the information that pipeline operators like Sunoco use to determine the worst case discharge. PHMSA provided no explanation whatsoever for concluding that disclosure of this kind of information no longer presents the security risks described in its 2014 policy.

Nor did PHMSA consider the obvious possibility that such risks are even greater today than they were in 2014. *See, e.g.*, Improving the Nation's Cybersecurity, Exec. Order No. 14,028, 86 Fed. Reg. 26,633 (May 17, 2021) ("The United States faces persistent and *increasingly* sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. . . . Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector." (emphasis added)); *see also* U.S. Gov't Accountability Off., GAO-21-105263, *Critical Infrastructure Protection: TSA Is Taking Steps to Address Some Pipeline Security Program Weaknesses* 4 (July 27, 2021) ("In addition to their vulnerability to physical attacks, pipelines are vulnerable to cyberattacks or intrusions due to their *increased* reliance on computerized systems and electronic data—particularly industrial control systems." (emphasis added)). In light of these shortcomings, the agency's application of Exemption 7(F) to Sunoco's modeling information was arbitrary and capricious.

B. The Agency Arbitrarily Concluded that Factual Safety Information Is Not "Commercial" Within the Meaning of Exemption 4

The agency also misapplied Exemption 4, which protects trade secrets and "confidential commercial information." 5 U.S.C. § 552(b)(4). As relevant to this motion,[8] PHMSA concluded that Exemption 4 does not apply to Sunoco's modeling data because the information was not "commercial." In the agency's view, "factual safety information . . . used by and for emergency response" could not qualify as commercial information. Compl. Ex. T at 4. But as the government's motion acknowledges, the D.C. Circuit has long held that Exemption 4 applies whenever "the provider of the information has a *commercial interest* in the information submitted to the agency." Mot. 8 (emphasis added) (quoting *Baker & Hostetler LLP v. U.S. Dep't of Com.*, 473 F.3d 312, 319 (D.C. Cir. 2006)). As the business disruptions caused by the Colonial Pipeline cyberattack demonstrate, a pipeline operator like Sunoco plainly has a "commercial interest" in minimizing the likelihood of a debilitating pipeline attack.

In addition, the D.C. Circuit has squarely held that companies have a "commercial interest" in information about the potential safety risks associated with their operations. In *Critical Mass Energy Project v. Nuclear Regulatory Commission*, 830 F.2d 278, 281 (D.C. Cir. 1987), the court held that nuclear power plant safety reports were "commercial" because the power plants' "commercial fortunes . . . could be materially affected by the disclosure of health and safety problems experienced during the operation of nuclear power facilities." *Id.*[9] So, too, here. Sunoco is a for-profit commercial enterprise engaged in, among other things, the transportation of natural

[8] The agency concluded that the pipeline information is neither commercial nor confidential within the meaning of Exemption 4. The government seeks dismissal only on the ground that the information is not commercial (*see* Mot. 7-11); the Chamber accordingly focuses on that issue.

[9] The en banc court vacated this opinion on other grounds, but explicitly "agree[d]" with the conclusion that the information was "commercial in nature." *Critical Mass*, 975 F.2d at 880.

gas liquids through its pipelines. Sunoco has a commercial interest in continuing to operate pipelines, and the disclosure of the potential consequences of a pipeline disruption directly implicates that interest.

Contrary to the agency's view, it is not relevant that Sunoco developed the information to satisfy "safety-related compliance obligations" imposed by the agency. Compl. Ex. T at 4. In *Public Citizen Health Research Group v. FDA*, 704 F.2d 1280, 1290 (D.C. Cir. 1983), the court held that health and safety data for medical products constituted commercial information, as the data would be "instrumental in gaining marketing approval." Manufacturers often gather this type of health and safety data for the express purpose of complying with requirements necessary to obtain (and maintain) government approvals, yet that fact does not undermine the "commercial" nature of the data. The agency thus erred in concluding that the pipeline information at issue here does not fall within Exemption 4.

III. The Government's Position Would Jeopardize Public Safety and the Government's Ability to Obtain Important Safety Information

If the Court construes FOIA's exemptions as narrowly as the government requests *and* precludes private parties from challenging agencies' disclosure decisions, there is no question that a greater amount of confidential, sensitive information will end up in the public domain. Those disclosures will have significant negative ramifications, both for public safety and (at least in cases where private parties voluntarily provide information to the government) for the government's continuing ability to obtain the information that everyone agrees is "vital" to its work. *Food Mktg. Inst. v. Argus Leader Media*, 139 S. Ct. 2356, 2366 (2019).

A. Disclosure Could Put Sensitive Information in the Hands of Malicious Actors

As explained, releasing sensitive pipeline data could facilitate and even encourage third parties' efforts to damage critical infrastructure and the surrounding communities. *See supra* pp.

7-9. The government has consistently recognized that "pipelines are vulnerable to physical attacks—including the use of firearms or explosives—largely due to their stationary nature, the volatility of transported products, and the dispersed nature of pipeline networks." GAO, *Critical Infrastructure Protection*, *supra*, at 4 n.12. These concerns are even more salient today. The Colonial Pipeline cyberattack "has elevated concern . . . about the security of the nation's energy pipelines and government programs to protect critical infrastructure." Cong. Rsch. Serv., IN11667, *Colonial Pipeline: The DarkSide Strikes* 1 (May 11, 2021).

The Transportation Security Administration ("TSA")—the agency with "primary oversight responsibility for the physical security and cybersecurity" of pipeline systems—has responded to the Colonial Pipeline attack by issuing two Security Directives that impose stricter requirements on pipeline operators. GAO, *Critical Infrastructure Protection*, *supra*, at 2, 12-13 (discussing May 2021 and July 2021 cybersecurity directives). For example, TSA now requires pipeline operators to "report cybersecurity incidents" to the government. Transp. Sec. Admin., Security Directive Pipeline-2021-01 1 (May 28, 2021), *available at* https://bit.ly/2XtQ9Kz. The agency also requires operators to "review their current activities against TSA's recommendations for pipeline cybersecurity to assess cyber risks, identify any gaps, develop remediation measures, and report the results" to TSA and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency. *Id.* The Security Directive expressly assures pipeline operators that "[a]ll information that must be reported" to these agencies under the directive "is sensitive security information subject to the protections of" TSA regulations, *id.* at 2, which generally prohibit the disclosure of sensitive security information under FOIA, *see* 49 C.F.R. § 1520.15(a), (b).

At a time when the government seeks to obtain more sensitive information from critical infrastructure operators than ever before *and* when TSA has acknowledged the need to guard that

information against public disclosure, the Court should not interpret FOIA's exemptions in a way that allows other agencies to expose similarly sensitive information to hostile actors.

B. Release of Sunoco's Data Would Undermine Incentives to Cooperate with Widespread Government Requests for Information

More broadly, the government's position threatens to undermine the ability of government agencies to make "intelligent, well informed decisions." *Critical Mass*, 975 F.2d at 878. In some cases, the government relies on its regulatory or investigatory authority to compel the production of information; here, for example, PHMSA requested Sunoco's pipeline hazard analyses during the course of a safety inspection. Compl. ¶ 17. But more often, the government obtains information only because companies, *e.g.*, *Sharyland Water Supply Corp. v. Block*, 755 F.2d 397, 398 (5th Cir. 1985), labor unions, *e.g.*, *Am. Airlines, Inc. v. Nat'l Mediation Bd.*, 588 F.2d 863, 864-85 (2d Cir. 1978), and other actors, *e.g.*, *Utah v. DOI*, 256 F.3d 967, 968-69 (10th Cir. 2001) (Indian tribes), choose to participate in federal programs, apply for government benefits, or otherwise cooperate with federal agencies in a broad variety of programs.

Many of these government programs require disclosures. Such programs include grants and loans, where private commercial information is used to determine eligibility. *See, e.g.*, *Sharyland Water Supply*, 755 F.2d at 398 (corporation had filed audit reports with Farmers Home Administration in order to obtain a loan). Such programs also include schemes for granting permission to operate on federal land. *See, e.g.*, *Nat'l Parks & Conservation Ass'n v. Morton*, 498 F.2d 765, 766-67 (D.C. Cir. 1974) (national park concessioners submitted financial records to obtain licenses to operate on federal land), *overruled on other grounds by Food Mktg. Inst.*, 139 S. Ct. at 2364; *Story of Stuff Project v. U.S. Forest Serv.*, 366 F. Supp. 3d 66, 74-75 (D.D.C. 2019) (water bottling company submitted proprietary maps and diagrams to obtain permit to operate transmission facility on federal land). And, of course, government programs that require

disclosures also include various regulatory approval programs. *See, e.g.*, *Henson v. HHS*, 892 F.3d 868 (7th Cir. 2018) (medical device company submitted information about manufacturing process in application for premarket approval); *United Techs. Corp.*, 102 F.3d at 689 (aircraft manufacturer submitted engine designs and specifications for agency approval); *Forest Cnty. Potawatomi Cmty. v. Zinke*, 278 F. Supp. 3d 181 (D.D.C. 2017) (contractor submitted projected revenues and other detailed financial information in application for Indian gaming license). Similarly, virtually any company that chooses to assist the government in implementing a program—even when no government benefit, permit, or regulatory approval is at issue—will be required to turn over information to the government as a condition of its participation.

Companies also often share information voluntarily to work with the government toward solving regulatory challenges, advancing policy initiatives, and protecting public safety. For example, Sunoco commissioned the modeling analyses at issue here in order to develop its integrity management plan for pipelines in densely populated areas. Compl. ¶ 20. Although federal pipeline safety regulations require operators to develop and implement these plans, *see* 49 C.F.R. §§ 192.911, 195.452, they do not require operators to regularly submit all of the data underlying their plans to government agencies. Nonetheless, Sunoco routinely shares this type of information with emergency response agencies voluntarily—*i.e.*, outside the context of any inspection or enforcement action—for emergency preparedness purposes, and subject to an explicit condition of confidentiality. *See* Opp'n 3.

Other federal agencies have established more formal information-sharing programs. For example, the Environmental Protection Agency has actively sought the participation of businesses in many information-sharing programs to promote important environmental goals. *See* Env't Prot. Agency, *Partnership Programs*, https://bit.ly/2Z9OiuP (last visited Oct. 22, 2021). The Federal

Aviation Administration has partnered with the unmanned aircraft industry to "share mutually beneficial information" regarding safety and operations. *See* Fed. Aviation Admin., *Partnership for Safety Plan Program*, https://bit.ly/3dnvITt (last updated Feb. 3, 2021). The Occupational Safety and Health Administration engages in voluntary strategic partnerships with employers "to identify the most serious workplace hazards, develop workplace-appropriate safety and health management systems, share resources, and find effective ways to reduce worker injuries, illnesses, and deaths." Occupational Safety & Health Admin, *Strategic Partnerships Overview*, https://bit.ly/3dsmJR9 (last visited Oct. 22, 2021). And PHMSA itself recently convened a working group to make recommendations for a voluntary information-sharing system for the pipeline industry. *See* PHMSA Fed. Advisory Comm., *Pipeline Safety Voluntary Information-Sharing System Recommendation Report* (Apr. 2019), *available at* https://bit.ly/3aUcOTF. The working group concluded that voluntary information sharing "is an essential element of an effective pipeline safety management program"—and also noted that any information-sharing system must "protect[] proprietary data" and "safety and security-sensitive information." *Id.* at 6.

If the Court accepts the government's invitation to weaken FOIA's protections, companies will be less likely to share confidential, sensitive information with the government through programs like these. The government often provides either express or implied assurances to companies that it will keep their information confidential, *see, e.g.*, *Food Mktg. Inst.*, 139 S. Ct. at 2363, but this case demonstrates that private parties cannot know in advance how far the government's commitment to confidentiality will extend. An agency may initially agree to keep information confidential, *see* Compl. Ex. K, yet change its mind after receiving a FOIA request or a FOIA appeal. Without the ability to challenge the agency's decision, companies are likely to assume that *any* information they provide—even the most sensitive commercial or security

information—cannot be protected from exposure to the public. That will inevitably discourage businesses from participating in voluntary government programs and initiatives whose success depends on robust cooperation with private industry. And even where the disclosure of information is mandatory, weakening FOIA's protections will significantly harm important government interests—in this case, by undermining the security of critical infrastructure.

CONCLUSION

The Court should deny Defendants' motion to dismiss.

Dated: October 22, 2021

Respectfully submitted,

/s/ John P. Elwood
John P. Elwood (D.C. Bar No. 452726)
Janine M. Lopez* (D.C. Bar No. 1685754)
ARNOLD & PORTER KAYE SCHOLER LLP
601 Massachusetts Avenue, NW
Washington, DC 20001
(202) 942-5000
John.Elwood@arnoldporter.com

Paul V. Lettow (D.C. Bar No. 502440)
Andrew R. Varcoe (D.C. Bar No. 473834)
U.S. CHAMBER LITIGATION CENTER
1615 H Street, NW
Washington, DC 20062
(202) 463-5337

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

Counsel for Amicus Curiae