IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

STANDING ROCK SIOUX TRIBE, Plaintiff, and CHEYENNE RIVER SIOUX TRIBE, Plaintiff-Intervenor, v. UNITED STATES ARMY CORPS OF ENGINEERS, Defendant, and DAKOTA ACCESS, LLC, Defendant-Intervenor and Cross-Claimant	Case No. 1:16-cv-01534 (JEB)

UNITED STATES ARMY CORPS OF ENGINEERS' OPPOSITION TO DAKOTA ACCESS, LLC'S MOTION FOR PROTECTIVE ORDER

Dakota Access, LLC seeks a protective order to prevent disclosure of certain portions of 11 documents in the administrative record of the Defendant, the United States Army Corps of Engineers ("Corps"). Dakota Access has proposed numerous redactions in those 11 documents, citing concerns that this information, if publicly released, could compromise the security of the Dakota Access pipeline. The Corps opposes Dakota Access's Motion for a Protective Order in part.

The Corps does not oppose a protective order prohibiting disclosure of information that would ordinarily be protected from disclosure by the Pipeline and Hazardous Materials Safety Administration ("PHMSA"). But the Corps does oppose redacting or otherwise withholding from

public release the remainder of the material Dakota Access has designated. These documents are part of the Corps' administrative record and should be available to the parties in this litigation and to the public. The Transportation Security Administration ("TSA"), the agency with expertise in identifying and protecting Sensitive Security Information ("SSI"), has concluded that the 11 documents do not contain any SSI. And Dakota Access has not met its burden of showing that the designated information should be withheld from disclosure either as Protected Critical Infrastructure Information ("PCII") or under Federal Rule of Civil Procedure 26(c).

In addition, the Corps opposes the inclusion of language in Dakota Access's proposed protective order that would require the Corps—indefinitely—to notify all of the parties, wait 10 days, and take additional steps before disclosing any protected information to third parties in response to a subpoena or other legal obligations. Such a provision is overbroad and imposes an undue burden on the Corps that is in addition to and may be inconsistent with independent federal statutory records management and production obligations. Instead, the provision should be stricken and the protective order should require the Plaintiffs to return or destroy all documents containing protected information within 10 days of a final, non-appealable judgment in this case.

I. BACKGROUND

A. Factual and Procedural Background

On November 10, 2016, the Corps lodged an administrative record for the July 25, 2016 decisions challenged by Plaintiff Standing Rock Sioux Tribe in its Complaint. ECF No. 55. As explained at the November 10, 2016 status conference, the Corps withheld from its production 31 documents in order to evaluate whether the documents contained pipeline security or culturally sensitive information protected from public disclosure and to attempt to resolve areas of disagreement between the parties on the scope of any such protections. On November 10, the

Court entered a Minute Order providing the parties until December 9, 2016, to address issues relating to the confidentiality of the Corps' administrative record.

Resolution of the record issues was delayed by multiple subsequent filings.[1] On February 1, 2017, however, Dakota Access filed a Motion for a Protective Order. ECF No. 92. In its Motion, Dakota Access sought to withhold from public disclosure certain information in 11 of the 31 documents originally withheld from the Corps' administrative record. Dakota Access argued that this information constituted critical infrastructure information and SSI and should not be publicly disclosed because it "could be used by terrorists or others intending to cause harm." Mot. Protective Order at 4-8.

As part of its confidentiality review of the documents in question, the Corps consulted with PHMSA and TSA. PHMSA is responsible for ensuring pipeline safety, and TSA is responsible for designating SSI. The Corps initially provided all 31 documents to PHMSA and TSA. After Dakota Access moved for a protective order, the Corps asked PHMSA and TSA to confirm their findings with respect to the 11 documents at issue in the Motion. *See* Declaration of David Lehman ¶¶ 3-4, attached as Exhibit 1 ("Lehman Decl."); Letter from D. Blair, TSA, to E. Zilioli, DOJ (Feb. 27, 2017), attached as Exhibit 2 ("TSA Letter").

[1] On November 15, 2016, Dakota Access filed a cross-claim against the Corps. ECF No. 57. On December 5, 2016, Dakota Access moved for summary judgment on its cross-claim. ECF No. 66. On December 7, 2016, Standing Rock and Cheyenne River proposed that their claims be stayed pending resolution of the cross-claim. ECF No. 67. Following the December 9, 2016 status conference, the Court issued a Minute Order setting an expedited schedule to resolve Dakota Access's motion for summary judgment. On December 16, 2016, Standing Rock, Cheyenne River, and the Corps formally moved to hold the Tribes' claims in abeyance, ECF No. 71, which this Court granted the same day, ECF No. 72.

After reviewing the 11 documents at issue in Dakota Access' Motion for Protective Order, TSA concluded that there was no SSI in these documents. *See* TSA Letter at 1. PHMSA concluded that some information marked for protection by Dakota Access in five of the documents[2] was consistent with information PHMSA would redact from public disclosure pursuant to 49 U.S.C. § 60138 and 5 U.S.C. § 552(b)(3), (b)(7)(F).[3] *See* Lehman Decl. ¶ 5. Exhibit A to the Lehman Declaration (which will be submitted under seal) contains approximately 50 proposed redactions of information designated by Dakota Access that PHMSA would also withhold from public disclosure in those five documents (the "Exhibit A Information"). *See id.* ¶ 7 & Ex. A. The remainder of those five documents and the other six documents[4] contained no information that PHMSA would protect from public disclosure under its redaction authorities. *See id.* ¶¶ 3-6.

B. Legal Framework

1. Sensitive Security Information

Congress has directed TSA to "prescribe regulations prohibiting the disclosure of information obtained or developed in carrying out security . . . if [TSA] decides that disclosing the information would . . . be detrimental to the security of transportation."[5] 49 U.S.C. §

---

[2] The five documents include: AR 12398-418, AR 12419-39, AR 12440-61, AR 74092-110, and AR 74713-29.

[3] 5 U.S.C. section 552(b)(3) and (b)(7)(F) are exemptions from the release of agency records under the Freedom of Information Act ("FOIA") for information exempted from disclosure by statute and information pertaining to law enforcement, respectively.

[4] The six documents include: AR 12462-76, AR 12477-93, AR 12494-511, AR 67857-94, AR 74733-46, and AR 74747-60.

[5] 49 U.S.C. § 114 refers to TSA's Administrator as "the Under Secretary of Transportation for Security" because TSA was originally a part of the Department of Transportation. The functions of TSA and the Under Secretary of Transportation for Security were transferred to the Department of Homeland Security pursuant to section 403(2) of the Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135, 2178 (codified at 6 U.S.C. § 203(2)). The Under Secretary is now known as the Administrator of TSA. *See* 49 C.F.R. § 1500.3.

114(r)(1)(C). In accordance with its statutory mandate, TSA adopted regulations regarding the protection of SSI. *See* 49 C.F.R. Part 1520. Under TSA's regulations, SSI includes "information obtained or developed in the conduct of security activities, including research and development, the disclosure of which TSA has determined would . . . [b]e detrimental to the security of transportation." 49 C.F.R. § 1520.5(a)(3). 49 C.F.R. § 1520.5(b) sets forth certain categories of information that can constitute SSI. But information falling within those categories "does not automatically constitute SSI." *Robinson v. Napolitano*, 689 F.3d 888, 893 n.2 (8th Cir. 2012). In order for information to constitute SSI, TSA must *also* determine that the information was "obtained or developed in the conduct of security activities" and that disclosure of the information would "[b]e detrimental to the security of transportation." *Id.*; 49 C.F.R. § 1520.5(a)(3). The TSA Administrator has delegated authority to make SSI determinations to the Chief of TSA's SSI Program. *See Lacson v. DHS*, 726 F.3d 170, 173 n.1 (D.C. Cir. 2013).

Covered persons are authorized to have access to SSI but have an express duty to protect the information. 49 C.F.R. § 1520.9. Such persons must "[t]ake reasonable steps to safeguard SSI . . . from unauthorized disclosure" and "[r]efer requests by other persons for SSI to TSA . . . ." *Id.* § 1520.9(a). Violation of these and additional non-disclosure requirements "is grounds for a civil penalty and other enforcement or corrective action . . . ." *Id.* § 1520.17.

2. Protected Critical Infrastructure Information

Congress enacted the Critical Infrastructures Protection Act of 2001 to ensure "the reliable provision of cyber and physical infrastructure services critical to maintaining the national defense, continuity of government, economic prosperity, and quality of life in the United States." 42 U.S.C. § 5195c(b)(3). *Critical infrastructure* is defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets

would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." *Id*. § 5195c(e). The statute created a National Infrastructure Simulation and Analysis Center, which was tasked with, among other things, modeling and simulating critical infrastructures in order to enhance their stability and prevent disruptions in continuity of their operations. *Id*. § 5195c(d). The statute does not prohibit the public disclosure of any information concerning critical infrastructures.

The Critical Infrastructure Information Act of 2002 established the Protected Critical Infrastructure Information Program to protect from public disclosure private infrastructure information voluntarily shared with the federal government. *See* 6 U.S.C. § 133. The U.S. Department of Homeland Security ("DHS") has exclusive authority to designate information as PCII and has established regulations setting forth procedures for the proper handling of PCII by federal agencies. *See* 6 C.F.R. Part 29. Information only receives the protections of PCII if it meets the requirements of 6 C.F.R. § 29.5, including, among other things, that it be submitted voluntarily to the DHS PCII Program and be labeled with the following statement: "This information is voluntarily submitted to the Federal government in expectation of protection from disclosure as provided by the provisions of the Critical Infrastructure Information Act of 2002."

3. Pipeline Response Plans

In accordance with the Pipeline Safety, Regulatory Certainty, and Job Creation Act of 2011, the Department of Transportation maintains copies of response plans for onshore oil pipelines.[6] *See*

[6] A response plan is defined as "the operator's core plan and the response zone appendices for responding, to the maximum extent practicable, to a worse case discharge of oil, or the substantial threat of such a discharge." 49 C.F.R. § 194.5. PHMSA is responsible for reviewing and approving response plans. 49 C.F.R. § 194.119.

49 U.S.C. § 60138(a)(1). The Department must provide a copy of a response plan upon request but may exclude from the released copy, if deemed appropriate:

> (A) proprietary information; (B) security-sensitive information, including information described in [49 C.F.R. § 1520.5(a)]; (C) specific response resources and tactical resource deployment plans; and (D) the specific amount and location of worst case discharges (as defined in [49 C.F.R. part 194]), including the process by which an owner or operator determines the worst case discharge.

49 U.S.C. § 60138(a)(2)(A)-(D).

II. STANDARD OF REVIEW

> Under Rule 26(c) of the Federal Rules of Civil Procedure, a District Court
>
> may, for good cause, issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense, including . . .
>
> (G) requiring that a trade secret or other confidential research, development, or commercial information not be revealed or be revealed only in a specified way . . .

Fed. R. Civ. P. 26(c)(1)(G). The party seeking a protective order carries the burden of establishing that a protective order should be granted. *Doe v. Provident Life & Accident Ins. Co*., 247 F.R.D. 218, 221 (D.D.C. 2008) (citation omitted). The movant "must establish 'good cause' under Rule 26(c) 'by demonstrating the specific evidence of the harm that would result. . . .'" *Id.* (quoting *Jennings v. Family Mgmt*., 201 F.R.D. 272, 275 (D.D.C. 2001)). In particular, the movant "must articulate specific facts to support its request and cannot rely on speculative or conclusory statements." *Jennings*, 201 F.R.D. at 275 (citations omitted). This Court employs a balancing test in determining whether to grant a motion for protective order, "weighing the burdensomeness to the moving party against the requestor's need for, and relevance of the information sought." *Doe*, 247 F.R.D. at 221 (citations omitted).

III. ARGUMENT

Relying on the expertise of agencies charged with implementing laws and regulations designed to protect the security of infrastructure projects, the Corps agrees that a *limited* amount of

information designated by Dakota Access in five documents in the Corps' administrative record should be protected from public disclosure. *See* Lehman Decl. Ex. A. Thus, the Corps does not oppose the entry of a protective order covering the Exhibit A Information. However, a protective order covering the remaining information designated by Dakota Access in its Motion is not appropriate, because Dakota Access has not met its burden of establishing that it warrants protection.

Regardless of the scope of information subject to the protective order, the Corps requests that paragraph 11 in the proposed order be stricken, at least as to the Corps. This provision, which would require the Corps—indefinitely—to notify Dakota Access and the Tribes before releasing any information subject to the protective order in response to a subpoena or other legal obligation, is overbroad and would impose an undue burden on the Corps that is in addition to and potentially inconsistent with existing statutory records management obligations.

A. A Protective Order Is Not Warranted for the Majority of Dakota Access's Designations.

Dakota Access argues that a protective order is required for numerous portions of the 11 documents in question because that information is—in Dakota Access's opinion—SSI and PCII likely to aid terrorism. The motion should be denied, however, because the agency responsible for identifying and ensuring the protection of SSI has concluded that none is present in these documents and Dakota Access has not established that the documents contain PCII or should otherwise be protected.

1. The Documents Do Not Contain SSI.

Dakota Access first asserts that the designated information constitutes SSI and warrants protection under 49 U.S.C. § 114(r) and 49 C.F.R. § 1520.5. Mot. Protective Order at 2. It is not necessary for the Court to reach this issue, because TSA, which has authority to decide what information constitutes and does not constitute SSI, has reviewed the subject documents and

determined they do not contain any SSI. *See* TSA Letter. Specifically, the Chief of TSA's SSI Program, which is responsible for conducting assessments and reviews of records to determine which information contained therein is SSI, if any, personally reviewed the 11 documents attached to Dakota Access's Motion for Protective Order. *Id*. He determined they do not contain SSI. *Id*.

TSA retains broad discretion to determine what information does and does not constitute SSI. *See, e.g., Ibrahim v. DHS*, No. C 06-00545, 2009 WL 5069133, at *7 (N.D. Cal. Dec. 17, 2009). Whether to designate information as SSI is a question for TSA and is not within the purview of covered persons who are authorized to access SSI, such as Dakota Access. Also, this Court would not have jurisdiction to consider whether the information should be protected as SSI, as Congress has vested exclusive jurisdiction in the United States Courts of Appeals to review TSA's SSI determinations. *See* 49 U.S.C. § 46110(a), (c)[7]; *see, e.g., Elec. Privacy Info. Ctr. v. DHS*, 928 F. Supp. 2d 139, 146-47 (D.D.C. 2013) ("[D]istrict courts may not review TSA orders that designate material as sensitive security information.") (citation omitted).

In sum, it is unnecessary for this Court to consider Dakota Access's claim that the information should be protected as SSI.

2. The Documents Do Not Contain PCII.

Dakota Access also asserts that "certain details" in the 11 documents "constitute Critical Infrastructure Information" and should be protected under 42 U.S.C. § 5195c. Mot. Protective Order at 2, 7-8. The company reasons that its pipeline is "part of the national critical physical

[7] 49 U.S.C. § 46110 actually references SSI determinations made under 49 U.S.C. § 114(s), which was the former statutory provision regarding SSI determinations. In 2007, 49 U.S.C. § 114(s) was redesignated as § 114(r), but 49 U.S.C. § 46110 has not yet been updated to reflect that clerical change. Since 2007, courts have recognized that 49 U.S.C. § 46110 applies to orders designating material as SSI. *See, e.g., Lacson v. DHS*, 726 F.3d 170, 173-77 (D.C. Cir. 2013).

infrastructure" and that the public release of the designated information in the documents in question might compromise the pipeline. *Id*. at 8. Dakota Access's vague reasoning could apply to virtually any map of the pipeline's route and most documents in the Corps' November 10, 2016 administrative record. But regardless of whether the designated information pertains to critical infrastructures, 42 U.S.C. § 5195c does not define much less prohibit the disclosure of "critical infrastructure information"; the law merely establishes an organization to study ways to protect critical infrastructures. Thus, it offers no basis for a protective order here.

To the extent Dakota Access meant to argue that the information constitutes PCII, the company has not alleged, much less established, that the information met the strict requirements of 6 C.F.R. § 29.5. For example, a quick glance at the 11 documents makes clear that they do not contain the express statement required under that regulation, and Dakota Access has not alleged that the company submitted the documents to the PCII Program within DHS for inclusion in the program.

3. The Designated Information Should Not Be Treated as Confidential.

Finally, Dakota Access has not met its burden under the Court's balancing test for protective orders under Fed. R. Civ. P. 26(c) to establish why the designated information must be kept confidential. First, there is a need for the information, and it is relevant to the litigation. The information is part of the Corps' administrative record for the agency actions challenged in this case. It is not within Dakota Access's judgment to determine whether the designated information is relevant to the litigation, particularly at the early stages of merits briefing. *See* Mot. Protective Order at 10. And since the documents in question are part of the Corps' records, there is an interest in making the information publicly available. *See, e.g., Chiquita Brands Int'l, Inc. v. SEC*, 805 F.3d 289, 294 (D.C. Cir. 2015) (holding in FOIA case that there is a "strong presumption in favor of disclosure") (citation omitted).

Second, Dakota Access has not provided any facts or evidence establishing that it will be harmed by the release of the designated material. As this Court explained in *Jennings v. Family Management*, Dakota Access cannot rely on mere speculation that the information might be used to cause harm to the company or its pipeline. 201 F.R.D. at 275. Significantly, much of the designated information in the 11 documents is already publicly available, such as the names of water bodies and counties where the pipeline crosses. *E.g.*, AR 12398-418, AR 12440-61, AR 12462-67, AR 12477-81, AR 12494-98, AR 67858, AR 74092-110, AR 74733-36, AR 74747-50. Dakota Access argues that even if this information is already in the public domain, it can still be damaging when available "in conjunction with other information . . . ." Mot. Protective Order at 9 n.7. But Dakota Access has not provided any concrete examples where this might occur, instead relying on a single article discussing concerns about terrorist threats to railroad shipments. *See id.* at Ex. B.

In conclusion, a protective order is not warranted for any information in the 11 documents other than the Exhibit A Information.

B. The Requirement to Notify Parties Before Disclosing Protected Information Should Be Stricken.

Paragraph 11 of the proposed protective order would require "any party", including the Corps, to notify all of the parties and wait 10 days before disclosing any protected information to third parties in response to a subpoena or other legal obligations. *See* ECF No. 92-4 ¶ 11. The paragraph would also require the Corps to "take reasonable steps" to protect the information consistent with the protective order. *Id.* The paragraph should be stricken as to the Corps, because it is overbroad and imposes an undue burden on the Corps that is in addition to and potentially inconsistent with existing statutory records management obligations. Indeed, these documents are in the Corps' possession as a result of its obligations as the agency that made the decisions that are challenged in this case. The Corps did not obtain these documents as a result of or through this

litigation. The Corps has various statutory obligations with respect to the management—including preservation and protection—of these documents. Dakota Access's motion effectively seeks to create new obligations on the Corps even though the Corps did not obtain these documents in the litigation and despite the Corps' statutory obligations with respect to the documents. There is simply no basis to add documentary burdens to the Corps when the agency is properly in possession of the documents outside of the litigation context.

Obligations that continue after final judgement tax judicial resources and the resources of the Corps unduly because the United States could be subject to lawsuits seeking this information years in the future, long after a final judgment in this case, when the personnel familiar with this matter are no longer available. Compliance with this proposed paragraph would require the agencies with jurisdiction over federal records to modify their processes for handling this class of federal records to keep individuals aware of this additional, extra-statutory requirement. This burdensome requirement is not warranted here.

The proposed paragraph may also conflict with the existing statutory requirements to manage federal records. The United States and its agencies, including the Corps, must maintain and produce documents pursuant to statutes including the Federal Records Act, 44 U.S.C. §§ 3101-07, 3301-14, FOIA, 5 U.S.C. § 552, and the Privacy Act, 5 U.S.C. § 552a. To the extent documents contain SSI or other information raising security concerns, agencies must abide by additional legal requirements. *See, e.g.*, 49 C.F.R. § 1520.15. The Corps obtained the 11 documents in question during the course of considering Dakota Access's requested pipeline crossings. The Corps must maintain these documents in accordance with its statutory obligations independent of this litigation. Thus, the proposed requirement that the Corps take steps to protect the information in accordance with the

protective order may conflict with, for example, an obligation to produce the documents in response to a FOIA request.

Instead, the Corps proposes that the Plaintiffs (who, in contrast to the Corps, only obtained and need to use the documents in this litigation) return or destroy all documents containing protected information, including any court filings referencing the protected information, within 10 days of a final, non-appealable judgment in this case. The Corps will continue to maintain the documents in accordance with its legal obligations. This should obviate the need for the proposed paragraph 11.

IV. CONCLUSION

Dakota Access' Motion for a Protective Order should be granted with respect to the approximately 50 proposed redactions identified by PHMSA in Exhibit A to the Lehman Declaration. The motion should be denied with respect to the remaining redactions proposed by Dakota Access. If the Court enters a protective order, the Corps requests that the proposed paragraph 11 requiring the Corps to notify the other parties and wait 10 days before disclosing any protected information to third parties in response to a subpoena or other legal obligation be stricken and be followed by a requirement that, within 10 days of a final judgment, the Plaintiffs destroy or return all documents containing protected information prepared or used during this litigation.

Dated: March 1, 2017

Respectfully submitted,

JEFFREY H. WOOD
Acting Assistant Attorney General
Environment and Natural Resources Division

By: /s/ *Erica Zilioli*
MATTHEW MARINELLI, IL Bar 6277967
REUBEN S. SCHIFMAN, NY Bar
AMARVEER S. BRAR, CA Bar 309615
U.S. Department of Justice
Natural Resources Section

P.O. Box 7611
Benjamin Franklin Station
Washington, DC 20044
Phone: (202) 305-0293 (Marinelli)
Phone: (202) 305-4224 (Schifman)
Phone: (202) 305-0479 (Brar)
Fax: (202) 305-0506
matthew.marinelli@usdoj.gov
reuben.schifman@usdoj.gov
amarveer.brar@usdoj.gov

ERICA M. ZILIOLI, D.C. Bar 488073
U.S. Department of Justice
Environmental Defense Section
P.O. Box 7611
Washington, DC 20044
Phone: (202) 514-6390
Fax: (202) 514-8865
erica.zilioli@usdoj.gov

Attorneys for the United States Army Corps of Engineers

OF COUNSEL:

MILTON BOYD
MELANIE CASNER
U.S. Army Corps of Engineers
Office of Chief Counsel
Washington, DC

CERTIFICATE OF SERVICE

I hereby certify that, on the 1st day of March, 2017, a copy of the foregoing was filed through the Court's CM/ECF management system and electronically served on counsel of record.

/s/ *Erica Zilioli*

Erica M. Zilioli