

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

COMPETITIVE ENTERPRISE INSTITUTE,
et al.,

Petitioner,

v.

TRANSPORTATION SECURITY
ADMINISTRATION,

Respondent.

Nos. 16-1135 & -1139

**MOTION TO FILE PORTIONS OF THE ADMINISTRATIVE RECORD
UNDER SEAL AND PORTIONS OF THE ADMINISTRATIVE RECORD
UNDER SEAL AND *EX PARTE***

The administrative record in this case consists of certain materials that are contained in a public rulemaking docket, and additional materials that are not available in the public docket because they were not appropriate for public filing. Respondents respectfully move for leave to file under seal a volume of copyrighted/proprietary documents and a volume of documents that contain For Official Use Only information. Respondents also move to file under seal and *ex parte* four volumes of the Administrative Record that contain Sensitive Security Information. In support of the motion, counsel states as follows:

1. The consolidated petitions for review challenge the Transportation Security Administration (TSA) final rule regarding passenger screening using Advanced Imaging Technology, or AIT. *See Passenger Screening Using Advanced Imaging*

Technology, 81 Fed. Reg. 11,363 (2016). The rule was adopted through a formal notice-and-comment rulemaking process.

2. The public rulemaking docket contains the public materials that are part of the Administrative Record, which are available at <https://www.regulations.gov/docket?D=TSA-2013-0004>. TSA has filed a certified index of record to the public materials.

3. The Administrative Record also contains additional material that was considered by TSA in the course of the rulemaking process that is not appropriate for public filing and is not available in the public rulemaking docket.

4. Volume 2 of the Administrative Record contains information that is copyrighted and was provided to TSA under a single-use license, or that is proprietary information. TSA respectfully requests that the Court file this volume under seal. Similar material was permitted to be filed under seal by the Court in *Electronic Privacy Information Ctr. v. DHS*, No. 10-1157 (D.C. Cir.). See *Electronic Privacy Information Ctr. v. DHS*, No. 10-1157, Order (D.C. Cir. Feb. 22, 2011).

5. Volume 3 of the Administrative Record contains information that is For Official Use Only. As explained in the attached declaration, those documents set forth risks to and vulnerabilities of the Nation's security infrastructure. See Declaration of Thomas Francis ¶¶ 10-11. Terrorists and other wrongdoers could

exploit those evaluations to harm the national security. TSA respectfully requests that this volume should also be filed under seal. Filing this material under seal will ensure that petitioners and their counsel do not publicly disclose it. *See* D.C. Cir. Rule 47.1(a) (“Parties and their counsel are responsible for assuring that materials under seal remain under seal and are not publicly disclosed.”).

6. Copies of Volumes 2 and 3 of the Administrative Record will be served on counsel for petitioners if the Court grants the motion, and petitioners and their counsel are required to handle the material in accordance with D.C. Circuit Rule 47.1(a).

6. Volumes 4A-4D of the Administrative Record contain information that has been designated as Sensitive Security Information, or SSI. SSI is information the disclosure of which TSA has determined would “[b]e detrimental to the security of transportation.” 49 C.F.R. § 1520.5(a); *see* 49 U.S.C. § 114(r)(1)(C) (requiring TSA to prohibit the disclosure of information that “would . . . be detrimental to the security of transportation”). SSI may only be disclosed to a “covered person[]” with a “need to know” the information. *See* 49 C.F.R. § 1520.9(a)(1). Neither petitioners nor their counsel are “covered persons” with a “need to know” SSI within the meaning of the regulation. Accordingly, these volumes should be filed *ex parte* and under seal by the Court. This Court has previously allowed the government to file

SSI information in the administrative record *ex parte*. See *Jifry v. FAA*, 370 F.3d 1174, 1182 (D.C. Cir. 2004).

7. Volume 5 of the Administrative Record contains classified information. The handling of classified information is governed by federal law. See, e.g., Exec. Order No. 13,526; 75 Fed. Reg. 707 (Dec. 29, 2009). Federal law prohibits disclosure of classified information except to individuals who have been cleared for access to the information by the head of a federal agency or his designee; who have signed a nondisclosure agreement; and who have a need to know the information. See Exec. Order No. 13,526, § 4.1(a); 75 Fed. Reg. at 720. Accordingly, the classified portions of the record may not be disclosed to the public or to petitioners or their counsel, who have not been cleared for access to classified information. Volume 5 should be filed by the Court *ex parte* and under seal.

8. Counsel for TSA has consulted with counsel for petitioners, who have indicated that petitioners oppose this motion.

Respectfully submitted,

MARK B. STERN

/s/ Sharon Swingle

SHARON SWINGLE

(202) 353-2689

Attorneys, Appellate Staff

Civil Division, Room 7250

Department of Justice

950 Pennsylvania Ave., N.W.

Washington, D.C. 20530-0001

SEPTEMBER 2016

personal knowledge and information obtained by me in the course of my official duties.

2. The mission of OIA is to efficiently and effectively receive, assess, and distribute actionable intelligence and vetting information related to transportation security in order to equip security professionals focused on this sector with timely and relevant information needed to prevent or mitigate threats to transportation.

3. Within OIA, I serve as the principal intelligence expert for the Assistant Administrator and Deputy Assistant Administrator regarding the development and oversight of Trend Analysis, Situational Analysis, and Production Management.

4. Among the products for which my Division within OIA is responsible are Civil Aviation Threat Assessments (CATAs), which are issued regularly and evaluate the risks presented by various entities and the vulnerabilities that terrorists and others might seek to exploit in order to harm the civil air transportation network.

5. In order to ensure that OIA's CATAs are available to the wide array of security professionals, OIA has issued these documents in a non-classified format.

6. The level of analysis contained within OIA's CATAs is nevertheless very sensitive.
7. OIA has designated the CATA for 2008, issued on March 20, 2008, as containing information that is For Official Use Only (FOUO). OIA has designated the CATA for 2010, issued on June 1, 2010, as containing information that is FOUO, and TSA has further determined that this document also contains Sensitive Security Information (SSI) as defined by 49 U.S.C. § 114(r) and 49 C.F.R. part 1520. It is my understanding that the SSI in the CATA for 2010 has been redacted for purposes of inclusion in the under seal volume 3 of the administrative record in the above-captioned case. OIA has designated the CATA for 2011, issued on October 12, 2011, as containing information that is protected by the privilege for law enforcement sensitive (LES) information as well as information that is FOUO. It is my understanding that the LES information in the CATA for 2011 has been redacted from the version of the document included in volume 3 of the administrative record. I also understand that information identifying certain U.S. persons ("USPERs") has been redacted so that it is also omitted from this document altogether.
8. For all information designated as FOUO, a determination has been made that "the unauthorized disclosure of [the information] could adversely impact a

person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national interest." Department of Homeland Security, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*, Management Directive 11042.1, at 1 ¶ 4. Pursuant to the governing management directive, FOUO information must be handled, stored, disseminated, and transmitted in specified ways that safeguard the information. *See id.* at 6-12 ¶ 6(F)-(L). As relevant here, FOUO information may be distributed only to individuals with a need-to-know the information. *See id.* at 8-9 ¶ 6(H).

9. In determining that the CATAs for 2008, 2010, and 2011 should be designated as containing FOUO, OIA concluded that limited restrictions on the dissemination of these particular intelligence assessments struck the necessary balance between ensuring that these vital products were sufficiently available to transportation security professionals, yet were not freely available to those who might exploit the analysis and assessment contained therein to undermine transportation security.

10. The unrestricted dissemination of CATAs presents the real possibility that those intending to disrupt the nation's civil aviation transportation system will be able to evaluate not only TSA's perceived weaknesses, but also the extent to which TSA appears to be aware of their organizations and activities.

11. Unrestricted dissemination of CATAs could, therefore, create systemic vulnerabilities, by affording the entities identified therein a clearer understanding of TSA's analysis of threat information and priorities, as well as by degrading the information-sharing relationships TSA has developed with certain stakeholders.

12. In creating and distributing CATAs, OIA expects that those within TSA and TSA's partners will ensure that these products are not freely available and are handled in accordance with the Department of Homeland Security's Management Directive 11042.1 where applicable.

13. For these reasons, it is important that, notwithstanding their use in this litigation, the CATAs referenced in Paragraph 7 not be filed on the public docket unless further redacted to protect the information they contain that has been designated as FOUO. It is also important that Petitioners be prohibited from disseminating the CATAs or any information contained therein, and that Petitioners treat the CATAs in accordance with the requirements outlined in the Department of Homeland Security's Management Directive 11042.1.

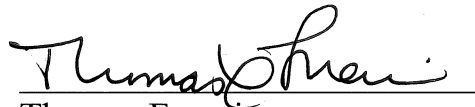
///

///

///

I declare under penalty of perjury that the foregoing is true and correct.

Executed September 15, 2016
Arlington, Virginia



Thomas Francis

Deputy Director, Threat Analysis Division
Office of Intelligence & Analysis
Transportation Security Administration
U.S. Department of Homeland Security

CERTIFICATE OF SERVICE

I hereby certify that on September 19, 2016, I electronically filed the foregoing Motion to File Portions of the Administrative Record Under Seal and Portions of the Administrative Record Under Seal and *Ex Parte* with the Clerk of the Court and served opposing counsel through the appellate CM/ECF system. Paper copies of Volumes 2, 3, and 4A-4D of the Administrative Record were lodged with the Court by hand delivery. Paper copies of Volume 5 of the Administrative Record were lodged with the Court through the Court Information Security Officer.

/s/ Sharon Swingle
SHARON SWINGLE
Counsel for Respondents