UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER **1718 Connecticut Ave., NW** **Suite 200** **Washington, DC 20009** **Plaintiff,**	)	
v.	)	**Civil Action No. _____**
U.S. CUSTOMS AND BORDER PROTECTION **1300 Pennsylvania Ave. NW** **Washington, DC 20229** **Defendant**	)	

COMPLAINT FOR INJUNCTIVE RELIEF

1. This is an action under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552 (2012), for injunctive and other appropriate relief, seeking the release of agency records requested by the Electronic Privacy Information Center ("EPIC") from Customs and Border Protection ("CBP") of the U.S. Department of Homeland Security ("DHS").

2. This lawsuit challenges the failure of CBP to disclose documents in response to EPIC's April 8, 2014 Freedom of Information Act request ("EPIC's FOIA Request"). EPIC's FOIA Request sought CBP records pertaining to the Analytical Framework for Intelligence ("AFI"). EPIC has constructively exhausted its administrative remedies. EPIC asks the Court to order immediate disclosure of all responsive records.

Jurisdiction and Venue

3. This Court has subject matter jurisdiction over this action and personal jurisdiction over the parties pursuant to 5 U.S.C. § 552(a)(4)(A)(vii), 5 U.S.C. § 552(a)(4)(B), and 5 U.S.C. § 552(a)(6)(C)(i). This Court also has jurisdiction over this action pursuant to 28 U.S.C. § 1331 (2012). Venue is proper in this district under 5 U.S.C. § 552(a)(4)(B).

Parties

4. Plaintiff EPIC is a public interest research organization incorporated as a not-for-profit corporation in Washington, D.C. EPIC conducts oversight of government activities and policies and analyzes their impact on civil liberties and privacy interests. Among its other activities, EPIC publishes books, reports, and a bi-weekly electronic newsletter. EPIC also maintains two popular Internet sites, www.epic.org and www.privacy.org, which contain extensive information on current privacy issues, including documents obtained from federal agencies under the FOIA. EPIC routinely and systematically disseminates information to the public through these websites and other media outlets. This Court recognized EPIC's role as a representative of the news media in *EPIC v. Dep't of Defense,* 241 F. Supp. 2d. 5, 6 (D.D.C. 2003).

5. Defendant CBP is a component of DHS, which is a federal agency within the meaning of 5 U.S.C. § 552(f)(1), and is headquartered in Washington, D.C.

FACTS

A) Development of AFI

6. On June 1, 2012, the DHS released a public description of the "Analytical Framework for Intelligence." U.S. Dep't of Homeland Sec., Privacy Impact Assessment for the Analytical Framework for Intelligence (2012).[1]

[1] *Available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_afi_june_2012.pdf.

7. According to the DHS, the AFI allows CPB to identify individuals, associations, relationships, and cargo "that may pose a potential law enforcement or security risk"; to prevent "the illegal entry of people and goods"; to conduct "additional research on persons and/or cargo" for patterns that indicate law enforcement or security risks; and to share final intelligence projects within DHS. *Id.* at 1.

8. Using AFI, CPB analysts search several government and non-government databases at once using automated processes, rather than manually entering search terms in each database. *Id.* at 2-4. Specifically, "AFI performs searches for and accesses information collected and maintained in other systems, including information from both government owned sources and commercial data aggregators." *Id.* at 9.

9. According to the DHS, "AFI does not collect information directly from individuals, but rather accesses information collected, generated, and stored by and in other systems." *Id*. at 10.

10. AFI maintains six categories of data, each of which contains personally identifiable information: DHS-owned data, other government agency data, information from commercial data aggregators, analyst-created data, analyst-provided data, and index information. *Id.* at 9-10.

11. AFI "collects identity and imagery data from several commercial data aggregators. . . [to] cross-reference that information with the information contained in DHS-owned systems." *Id.* at 10.

12. The Analytic Framework for Intelligence includes a vast amount of personally identifiable information, such as full name, address, age, gender, race, physical characteristics, marital status, residency status, country of citizenship, city and country of birth, date of birth,

Social Security Number, vehicle information, travel information, document information, passport information, law enforcement records, and familial and other contact information. *Id* at 9, 27-28.

13. Using AFI, CBP analysts conduct link analysis, anomaly detection, change detection analysis, temporal analysis, pattern analysis, and predictive modeling. IT Law Wiki, "Analytical Framework for Intelligence."[2]

14. AFI became operational in August 2012. U.S. Dep't of Homeland Sec., 2013 Data Mining Report to Congress 30 (2014).[3] In 2013, AFI initiated a pilot program to "enable analysts to view secret and [Sensitive But Unclassified] data on the same screens." *Id.*at 25.

15. To support the development of this program, CBP allocated $51.5 million between 2011 and 2013. Mickey McCarter, *Federal/State/Local Nebraska Ave.: Looking Ahead In DHS IT*, HSToday (Aug. 20, 2012).[4]

16. Since January 1, 2013, CBP has awarded contracts related to AFI totaling $178.2 million. CBP, Analytical Framework for Intelligence, ITDashboard.gov (last visited June 16, 2014).[5]

17. The DHS Privacy Office initiated a Privacy Compliance Report in August of 2013. Privacy Office, U.S. Dep't of Homeland Sec., 2013 Data Mining Report to Congress, 31 (Feb. 2014).[6]

18. Substantial concerns have been raised about the development of AFI, including sourcing data created within other CBP systems, data sharing, and privacy issues. The agency Chief Information Officer reported several times that, "PIA [Privacy Impact Assessment] and

[2] http://itlaw.wikia.com/wiki/Analytical_Framework_for_Intelligence
[3] *Available at* http://www.dhs.gov/sites/default/files/publications/dhs-privacy-2013-dhs-data-mining-report.pdf.
[4] *Available at* http://www.hstoday.us/channels/federalstatelocal/single-article-page/nebraska-ave-looking-ahead-in-dhs-it/735e462b9d2c3a2f9a829f09fd5605b2.html.
[5] *Available at* https://www.itdashboard.gov/investment/contracts/315.
[6] *Available at* http://www.dhs.gov/sites/default/files/publications/dhs-privacy-2013-dhs-data-mining-report.pdf

SORN [System of Records Notice] must be completed before the pilot can commence." *CBP - Analytical Framework for Intelligence: Evaluation History*, ITDashboard.gov (last visited July 18, 2014).[7]

19. The program also "permits DHS AFI analysts to upload and share information that may be relevant from other sources, such as the Internet or traditional news media, into projects, responses to [Requests for Information] RFIs, or final intelligence products." Privacy Impact Assessment for the Analytical Framework for Intelligence, *supra*, at 3.

20. Individuals have strong expressive interests in their online activity. If expressive activity is used as the basis for increased scrutiny at the border, serious First Amendment concerns may be implicated. The public should be informed about what types of information are being uploaded, from what sources, and how such information is being used.

B) AFI and Secret Risk-Based Profiles Assigned to US Citizens

21. Some of the data for AFI comes from the Automated Targeting System ("ATS"), which is also operated by the DHS. *Id*.

22. According to DHS, DHS and CBP use individual information within ATS to make "risk assessments" on individuals that travel to, through, and from the United States or "other locations where CBP maintains an enforcement or operational presence by land, air, or sea." Privacy Act of 1974; U.S. Customs and Border Protection, DHS/CBP–006—Automated Targeting System, System of Records, 77 Fed. Reg. 30,297-99 (proposed May 22, 2012). These risk assessments are assigned to U.S. citizens. Privacy Act of 1974; U.S. Customs and Border Protection, DHS/CBP—006—Automated Targeting System, System of Records, 77 Fed. Reg. 30, 297 - 99 (proposed May 22, 2012).

[7] https://www.itdashboard.gov/investment/evaluation-history/315

23. CBP uses ATS risk assessments to "signal to CBP officers that further inspection of a person, shipment, or conveyance may be warranted, even though an individual may not have been previously associated with a law enforcement action or otherwise be noted as a person of concern to law enforcement." U.S. Dep't of Homeland Sec., DHS/CBP/PIA-006 (b), Privacy Impact Assessment for the Automated Targeting System 19 (2012).[8]

24. CBP uses initial "risk-based" assessment matches and subsequent matches "to confirm continued official interest in the identified person." *Id.*

25. CBP uses a variety of personally identifiable information within ATS to perform risk assessments, including name, address, Social Security number, gender, nationality, race, and biometric information. Privacy Act of 1974; U.S. Customs and Border Protection, DHS/CBP–006—Automated Targeting System, System of Records, 77 Fed. Reg. at 30,299.

26. ATS also contains information generated by CBP, including "law enforcement or intelligence information regarding an individual" and "risk-based rules developed by analysts to assess and identify high-risk cargo, conveyances, or travelers that should be subject to further scrutiny or examination." *Id*. at 30,300.

27. Individuals having information within ATS are not notified of their risk assessment because DHS has exempted ATS from the "notification, access, amendment, and certain accounting procedures of the Privacy Act [.]" *Id*. at 30,303.

28. CBP should make public the basis of the Automated Targeting System "risk assessments" within the Analytical Framework for Intelligence.

[8] *Available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats006b.pdf.

EPIC's April 8, 2014 FOIA Request

29. Paragraphs 1-28 above are hereby incorporated by reference as if set forth fully herein.

30. On April 8, 2014, EPIC submitted, via certified mail, a FOIA request to the CBP's FOIA Office seeking records regarding the operations and legal basis for the program.

31. EPIC's FOIA Request asked for the following agency records:

> (1) All AFI training modules, request forms, and similar final guidance documents that are used in, or will be used in, the operation of the program;
>
> (2) Any records, memos, opinions, communications, or other documents that discuss potential or actual sources of information not currently held in DHS databases, or potential or actual uses of information not currently held in DHS databases;
>
> (3) Any records, contracts, or other communications with commercial data aggregators regarding the AFI program; and
>
> (4) The Privacy Compliance Report initiated in August 2013 by the DHS Privacy Office.

32. In EPIC's FOIA Request, EPIC also sought "News Media" fee status as a "representative of the news media" under 5 U.S.C. § 552(a)(4)(A)(ii).

33. In EPIC's FOIA Request, EPIC further sought waiver of all duplication fees in accordance with 5 U.S.C. § 552(a)(4)(A)(iii), because disclosure of the records requested will contribute significantly to public understanding of the operations or activities of the government.

34. According to the United States Postal Service Certified Mail tracker, CBP received EPIC's request on April 11, 2014.

35. As of the date of the filing of this complaint, EPIC has not received any response from CPB.

EPIC Has Constructively Exhausted its Administrative Remedies

36. Paragraphs 1-35 above are hereby incorporated by reference as if set forth fully herein.

37. It has been 69 business days since EPIC's FOIA Request was received by CBP.

38. CBP has failed to make a determination about EPIC's FOIA Request within the twenty-day time period prescribed by 5 U.S.C. § 552(a)(6)(A)(i).

39. CBP's failure to respond within the twenty-day statutory limit constitutes a constructive denial of EPIC's request, 5 U.S.C. § 552(a)(6)(A)(i), and exhaustion of EPIC's administrative remedies, 5 U.S.C. § 552(a)(6)(C)(i).

Count I

Violation of FOIA: Failure to Comply With Statutory Deadlines

40. Paragraphs 1-39 above are hereby incorporated by reference as if set forth fully herein.

41. As described above, Defendant CBP's failure to respond to EPIC's Request violated the statutory deadline imposed by the FOIA set forth in 5 U.S.C. § 552 (a)(6)(A)(i).

42. EPIC has exhausted the applicable administrative remedies with respect to EPIC's FOIA Request. 5 U.S.C. § 552(a)(6)(C)(i).

43. EPIC is entitled to injunctive relief compelling the release and disclosure of the requested agency records

Count II

Violation of FOIA: Unlawful Withholding of Agency Records

44. Paragraphs 1-43 above are hereby incorporated by reference as if set forth fully herein.

45. As described above, CBP has failed to comply with statutory deadlines and failed to make responsive records available to EPIC.

46. As a result of CBP's unlawful delay, the agency has withheld responsive agency records from EPIC in violation of FOIA, 5 U.S.C. § 552(a)(3)(A).

47. EPIC has exhausted the applicable administrative remedies with respect to EPIC's FOIA Request. 5 U.S.C. § 552(a)(6)(C)(i).

48. EPIC is entitled to injunctive relief compelling the release and disclosure of the requested agency records.

Requested Relief

WHEREFORE, EPIC prays that this Court:

A. Order CBP to promptly disclose to Plaintiff responsive agency records;

B. Order CBP to file, within 20 days of the date of the Court's Order in this matter, a *Vaughn* index, and an affidavit: 1) identifying each document withheld from disclosure; 2) stating CBP's claimed statutory exemption as to each withheld document (or portion of a document); and 3) explaining why each withheld document is exempt from disclosure;

C. Award EPIC its costs and reasonable attorneys' fees incurred in this action pursuant to 5 U.S.C. § 552(a)(4)(E); and

D. Grant such other relief as the Court may deem just and proper.

Respectfully submitted,

Marc Rotenberg, D.C. Bar # 422825

By: ____/s/ Ginger McCall_____
Ginger McCall, D.C. Bar # 1001104
Khaliah Barnes, D.C. Bar # 1013978
ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009
(202) 483-1140 (telephone)
(202) 483-1248 (facsimile)

Dated: July 18, 2014