

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

_____)	
ELECTRONIC PRIVACY INFORMATION)	
CENTER,)	Civil Action No: 14-1217 (RBW)
)	
Plaintiff,)	
)	
v.)	
)	
CUSTOMS AND BORDER PROTECTION,)	
)	
Defendant.)	
_____)	

NOTICE OF FILING VAUGHN INDEX

Defendant, Customs and Border Protection (“Defendant”), through undersigned counsel, hereby submits the attached Vaughn Index of withheld documents in the above captioned matter. Defendant reserves the right to further amend and/or supplement the attached index if additional information becomes available.

Respectfully submitted,

CHANNING D. PHILLIPS , DC Bar # 415793
United States Attorney for the District of
Columbia

DANIEL F. VAN HORN, DC Bar # 924092
Chief, Civil Division

PATRICIA K. MCBRIDE, PA Bar # 54561
Assistant United States Attorney
Civil Division
555 4th Street, NW, Room E-4808
Washington, DC 20530
Tel: 202.252.7123
Fax: 202.252.2599

Email: patricia.mcbride@usdoj.gov

Attorneys for Defendant

Electronic Privacy Information Center v. U.S. Customs and Border Protection
 14-1217 (RBW) (D.D.C.)
 Vaughn Index for (b)(7)(E)

PLAINTIFF BATES NUMBER/ EXHIBIT	DOCUMENT TITLE	EXEMPTION CLAIMED	CLASSIFICATION OF REDACTED INFORMATION
Exh. 1, 000005-37	Module 1 6.0	(b)(7)(E)	Module 1 provides an overview of AFI, including detailed tutorials, screen shots, and instructor notes to teach the law enforcement trainee techniques related to AFI, including how to access the AFI system, how to navigate AFI and its different components, and how to input, change, edit, and delete information in the AFI system. Disclosure of this information could enable unauthorized users to gain access to the system and alter, add, or delete information altogether, thus destroying the integrity of the system and allowing the unauthorized user to circumvent the law and potentially disrupt law enforcement investigations and proceedings.
Exh. 1, 000038-74	Module 2 6.0	(b)(7)(E)	Module 2 of the training materials provides an overview of the search and results functions of AFI. The training includes detailed instructions on how to use AFI's search features and techniques, build searches in the system, and navigate the system. Module 2 contains screen shots of the AFI system that specifically highlight how to accomplish the above-stated functions of AFI. The training module provides techniques, short-cuts, and other instructor notes to facilitate access to the system. Disclosure of this information could enable unauthorized users to gain access to the system and alter, add, or delete information altogether, thus destroying the integrity of the system and allowing the unauthorized user to circumvent the law and potentially disrupt law enforcement investigations and proceedings.
Exh. 1, 000075-96	Module 3 6.0	(b)(7)(E)	Module 3 of the training materials provides in-depth and detailed instructions regarding how to use AFI throughout a request for information cycle. The module contains PowerPoint slides that

Electronic Privacy Information Center v. U.S. Customs and Border Protection
 14-1217 (RBW) (D.D.C.)
Vaughn Index for (b)(7)(E)

			demonstrate techniques on how to locate and search certain pages within AFI, how to create a request for information, and screen shots to educate the law enforcement trainee on how to navigate the system. Disclosure of this information could enable unauthorized users to gain access to the system and alter, add, or delete information altogether, thus destroying the integrity of the system and allowing the unauthorized user to circumvent the law and potentially disrupt law enforcement investigations and proceedings.
Exh. 1, 000097-115	Module 4 6.0	(b)(7)(E)	Module 4 of the training materials provides information on how to use AFI to develop “tasks,” which are an inherent function of the law enforcement system. Similar to Module 3, which provided information on requests for information, Module 4 describes techniques and contains screen shots of the system and detailed instructor notes explaining how to best use and navigate the system to facilitate the user’s law enforcement purpose. Disclosure of this information could enable unauthorized users to gain access to the system and alter, add, or delete information altogether, thus destroying the integrity of the system and allowing the unauthorized user to circumvent the law and potentially disrupt law enforcement investigations and proceedings.
Exh. 1, 000116-134	Module 5 6.0	(b)(7)(E)	Module 5 of the training materials provides information on techniques for using the AFI system to develop a particular tool called a “Product.” Similar to Modules 3 and 4, it provides a detailed narrative (along with accompanying screen shots) that guide the user through the various processes, procedures, and techniques associated with products. Disclosure of this information could enable unauthorized users to gain access to the system and alter, add, or delete information altogether, thus destroying the integrity of the system and allowing the

Electronic Privacy Information Center v. U.S. Customs and Border Protection
 14-1217 (RBW) (D.D.C.)
 Vaughn Index for (b)(7)(E)

			unauthorized user to circumvent the law and potentially disrupt law enforcement investigations and proceedings.
Exh. 1, 000135-164	Module 6 6.0	(b)(7)(E)	Module 6 of the training materials includes step-by-step instructions on how to use AFI's Projects application. Similar to Modules 3, 4, and 5, it provides a detailed narrative (along with accompanying screen shots) that guide the user through the various techniques, processes, and procedures associated with the use of AFI's Projects application. Disclosure of this information could enable unauthorized users to gain access to the system and alter, add, or delete information altogether, thus destroying the integrity of the system and allowing the unauthorized user to circumvent the law and potentially disrupt law enforcement investigations and proceedings.
Exh. 1, 000165	AFI Quick Reference Card	(b)(7)(E)	AFI Quick Reference Guide provides an overview of key elements and techniques which can be used by law enforcement officers within the AFI application. The guide also provides keyboard shortcuts and other techniques designed to assist in navigation of the AFI application. Disclosure of this information could enable unauthorized users to gain access to the system and alter, add, or delete information altogether, thus destroying the integrity of the system and allowing the unauthorized user to circumvent the law and potentially disrupt law enforcement investigations and proceedings.
Exh. 1, 000166	Palantir Quick Reference Card	(b)(7)(E)	Palantir Quick Reference Card provides an overview of key elements, techniques which can be used by law enforcement officers and related keyboard shortcuts designed to assist in navigation of the Palantir application within AFI. Disclosure of this information could enable unauthorized users to gain access to the system and alter, add, or delete information altogether, thus destroying the integrity of the system and allowing the

Electronic Privacy Information Center v. U.S. Customs and Border Protection
 14-1217 (RBW) (D.D.C.)
 Vaughn Index for (b)(7)(E)

			unauthorized user to circumvent the law and potentially disrupt law enforcement investigations and proceedings.
Exh. 1, 000167-183	AFI Analyst Training Practical Exercise Solutions	(b)(7)(E)	The "AFI Analyst Training Practical Exercise Solutions" contains the answers to the practical exercises used to test a law enforcement trainee's proficiency with using the key elements, techniques and functionalities within the AFI application. Disclosure of this information could enable unauthorized users to gain access to the system and alter, add, or delete information altogether, thus destroying the integrity of the system and allowing the unauthorized user to circumvent the law and potentially disrupt law enforcement investigations and proceedings. Disclosure of this information could also reasonably allow a person to recognize identifiers that law enforcement uses to query CBP databases. Criminals could then circumvent the law by developing countermeasures to the search techniques.
Exh. 1, 000184-203	Practical Exercises AFI Palantir	(b)(7)(E)	The "Practical Exercises AFI Palantir" document contains the practical exercises used to test a law enforcement trainee's proficiency with using the key elements, techniques, and functionalities within the AFI application. Disclosure of this information could enable unauthorized users to gain access to the system and alter, add, or delete information altogether, thus destroying the integrity of the system and allowing the unauthorized user to circumvent the law and potentially disrupt law enforcement investigations and proceedings. Disclosure of this information could also reasonably allow a person to recognize identifiers that law enforcement uses to query CBP databases. Criminals could then circumvent the law by developing countermeasures to the search techniques.

Electronic Privacy Information Center v. U.S. Customs and Border Protection
 14-1217 (RBW) (D.D.C.)
Vaughn Index for (b)(7)(E)

Exh. 1, 000204	How to Request AFI Access	(b)(7)(E)	The "How to Request AFI Access" document provides detailed instructions on how to request access to the system. Disclosure of this information could enable unauthorized users to gain access to the system and alter, add, or delete information altogether, thus destroying the integrity of the system and allowing the unauthorized user to circumvent the law and potentially disrupt law enforcement investigations and proceedings.
Exh. 1, 000205	Approving AFI Access	(b)(7)(E)	The "Approving AFI Access" document provides detailed instructions on how to approve access to the AFI application. Disclosure of this information could enable unauthorized users to gain access to the system and alter, add, or delete information altogether, thus destroying the integrity of the system and allowing the unauthorized user to circumvent the law and potentially disrupt law enforcement investigations and proceedings.
Exh. 1, 000206	Approving AFI Consumer Access	(b)(7)(E)	The "Approving AFI Consumer Access" document provides detailed instructions on how to approve access to the AFI application. Disclosure of this information could enable unauthorized users to gain access to the system and alter, add, or delete information altogether, thus destroying the integrity of the system and allowing the unauthorized user to circumvent the law and potentially disrupt law enforcement investigations and proceedings.
Exh. 1, 000207	How to Request AFI Consumer Access	(b)(7)(E)	The "How to Request AFI Consumer Access" document provides detailed instructions on how to request access to the system. Disclosure of this information could enable unauthorized users to gain access to the system and alter, add, or delete information altogether, thus destroying the integrity of the system and allowing the unauthorized user to circumvent the law and

Electronic Privacy Information Center v. U.S. Customs and Border Protection
 14-1217 (RBW) (D.D.C.)
 Vaughn Index for (b)(7)(E)

			potentially disrupt law enforcement investigations and proceedings.
Exh. 1, 000208	Options for Setting up AFI Supervisors	(b)(7)(E)	The "Options for Setting up AFI Supervisors" document provides detailed options for setting up AFI supervisor accounts to request access to the system. Disclosure of this information could enable unauthorized users to gain access to the system and alter, add, or delete information altogether, thus destroying the integrity of the system and allowing the unauthorized user to circumvent the law and potentially disrupt law enforcement investigations and proceedings.
Exh. 2, 000001-2	AFI Trifold	(b)(7)(E)	This document provides an overview of AFI, including detailed screen shots and instructions on how to access the AFI system, related techniques used by law enforcement officers, and how to navigate AFI and its different components. Disclosure of this information could enable unauthorized users to gain access to the system and alter, add, or delete information altogether, thus destroying the integrity of the system and allowing the unauthorized user to circumvent the law and potentially disrupt law enforcement investigations and proceedings.
Exh. 2, 000003-8	AFI Program Overview	(b)(7)(E)	This document provides an overview of AFI, including detailed screen shots and instructions on how to access the AFI system, related techniques used by law enforcement, and how to navigate AFI and its different components. Disclosure of this information could enable unauthorized users to gain access to the system and alter, add, or delete information altogether, thus destroying the integrity of the system and allowing the unauthorized user to circumvent the law and potentially disrupt law enforcement investigations and proceedings.
Exh. 2, 000009-10	AFI Operational	(b)(7)(E)	This document lays out in detail the operational security posture of AFI. Disclosure of this information could enable unauthorized users to

Electronic Privacy Information Center v. U.S. Customs and Border Protection
 14-1217 (RBW) (D.D.C.)
 Vaughn Index for (b)(7)(E)

	Status and Security		gain access to the system and alter, add, or delete information altogether, thus destroying the integrity of the system and allowing the unauthorized user to circumvent the law and potentially disrupt law enforcement investigations and proceedings.
Exh. 2, 000011-12	Summary of AFI Roles for Release	(b)(7)(E)	This Summary of AFI Roles provides an overview of AFI roles, including detailed capabilities, techniques, and usage of each AFI role. Disclosure of this information could enable unauthorized users to gain access to the system and alter, add, or delete information altogether, thus destroying the integrity of the system and allowing the unauthorized user to circumvent the law and potentially disrupt law enforcement investigations and proceedings.
Exh. 2, 000013-15	AFI User Security Access Definitions	(b)(7)(E)	The "User Security Access Definitions" document provides instructor notes to facilitate access to the system. Disclosure of this information could enable unauthorized users to gain access to the system and alter, add, or delete information altogether, thus destroying the integrity of the system and allowing the unauthorized user to circumvent the law and potentially disrupt law enforcement investigations and proceedings.
Exh. 2, 000016-33	Statement of Work	(b)(7)(E)	This Statement of Work identifies database-specific information identifying LexisNexis Products, the release of which would disclose the type of searches conducted, and the law enforcement techniques and methods by which data is searched, organized and reported. It also includes descriptions of security services and critical infrastructure, the release of which could reasonably allow a person to recognize technologies and infrastructure critical to safeguarding law enforcement information. Criminals could then circumvent the law by targeting these technologies and infrastructure that protect the information.

Electronic Privacy Information Center v. U.S. Customs and Border Protection
 14-1217 (RBW) (D.D.C.)
Vaughn Index for (b)(7)(E)

Exh. 2, 000034-49	Statement of Work	(b)(7)(E)	This Statement of Work identifies database-specific information identifying LexisNexis Products, the release of which would disclose the types of searches conducted, and the law enforcement techniques and methods by which data is searched, organized and reported. It also includes descriptions of security services, critical infrastructure, and encryption standards, the release of which could reasonably allow a person to recognize technologies and infrastructure critical to safeguarding law enforcement information. Criminals could then circumvent the law by targeting these technologies and infrastructure that protect the information.
Exh. 3, 000001-4	AFI Data Source Ranking Results	(b)(7)(E)	The "AFI Data Source Ranking Results" document is a summary of a stakeholder survey regarding potential data sources for ingestion into AFI. Disclosure of this information would give unauthorized persons insight into CBP operational and analytical techniques, tactics, and procedures. It could reasonably allow a person to recognize identifiers that law enforcement use to query CBP databases. Criminals could then circumvent the law by developing countermeasures to the search techniques.
Exh. 3, 000005	AFI Data Sources	(b)(7)(E)	"AFI Data Sources" contains information relating to the source of several different types of data that are available in AFI. The document explains how to search AFI for each source, and a description of data found in each source. Disclosure of this information would give unauthorized persons insight into CBP operational and analytical techniques, tactics, and procedures. It could reasonably allow a person to recognize identifiers that law enforcement use to query CBP databases. Criminals could then circumvent the law by developing countermeasures to the search techniques.

Electronic Privacy Information Center v. U.S. Customs and Border Protection
 14-1217 (RBW) (D.D.C.)
Vaughn Index for (b)(7)(E)

Exh. 3, 000006-7	AFI Data Sources	(b)(7)(E)	“AFI Data Sources” (separate from the above document) gives a detailed description of each data source and how it relates to AFI. It also describes where, specifically, in AFI the user would go to access the data source. Disclosure of this information would give unauthorized persons insight into CBP operational and analytical law enforcement techniques, tactics, and procedures. It could reasonably allow a person to recognize identifiers that law enforcement use to query CBP databases. Criminals could then circumvent the law by developing countermeasures to the search techniques.
Exh. 3, 000008	Prior to Training Checklist	(b)(7)(E)	The “AFI Pre-Training Checklist” document provides instructor notes on techniques to facilitate access to the system. Disclosure of this information could enable unauthorized users to gain access to the system and alter, add, or delete information altogether, thus destroying the integrity of the system and allowing the unauthorized user to circumvent the law and potentially disrupt law enforcement investigations and proceedings.
Exh. 3, 000009	AFI Pre-Training Check List	(b)(7)(E)	The “AFI Pre-Training Checklist” document provides instructor notes on techniques to facilitate access to the system. Disclosure of this information could enable unauthorized users to gain access to the system and alter, add, or delete information altogether, thus destroying the integrity of the system and allowing the unauthorized user to circumvent the law and potentially disrupt law enforcement investigations and proceedings.
Exh. 3, 000011	Training Day Checklist	(b)(7)(E)	The “Training Day Checklist” contains an internal e-mail address for operational questions related to AFI. The disclosure of this address could be used by an unauthorized person to circumvent the law by improperly seeking information about AFI, which could lead to the system becoming

Electronic Privacy Information Center v. U.S. Customs and Border Protection
 14-1217 (RBW) (D.D.C.)
 Vaughn Index for (b)(7)(E)

			compromised and law enforcement investigations and proceedings becoming disrupted.
Exh. 3, 000012-13	AFI Projects Meeting Minutes	(b)(7)(E)	The AFI Projects Meeting Minutes includes detailed CBP operational challenges, as well as decisions regarding how law enforcement officers may effectively use AFI's search features, build searches in the system, and techniques on navigating the system. Disclosure of this information could enable unauthorized users to gain access to the system and alter, add, or delete information altogether, thus destroying the integrity of the system and allowing the unauthorized user to circumvent the law and potentially disrupt law enforcement investigations and proceedings.
Exh. 3, 000014-18	Order for Supplies and Services 8/16/10	(b)(7)(E)	This document contains database-specific information identifying LexisNexis Products, the release of which would disclose law enforcement techniques and methods by which data is searched, organized and reported by CBP. This information is law enforcement sensitive information, because, when read as a whole with the rest of the Supply Order, it could reasonably allow a person to recognize identifiers that law enforcement uses to query LexisNexis databases via AFI. Criminals could then circumvent the law by developing countermeasures to the search techniques.
Exh. 3, 000019-24	Order for Supplies and Services 12/29/12	(b)(7)(E)	This document contains database-specific information identifying LexisNexis Products, the release of which would disclose law enforcement techniques and methods by which data is searched, organized and reported. This information is law enforcement sensitive information, because, when read as a whole with the rest of the Supply Order, it could reasonably allow a person to recognize identifiers that law enforcement uses to query LexisNexis databases via AFI. Criminals could then circumvent the law by developing countermeasures to the search techniques.

Electronic Privacy Information Center v. U.S. Customs and Border Protection
 14-1217 (RBW) (D.D.C.)
 Vaughn Index for (b)(7)(E)

Exh. 3, 000025-33	Order for Supplies and Services 12/19/12	(b)(7)(E)	This document contains database-specific information identifying LexisNexis Products, the release of which would disclose law enforcement techniques and methods by which data is searched, organized and reported. This information is law enforcement sensitive information, because, when read as a whole with the rest of the Supply Order, it could reasonably allow a person to recognize identifiers that law enforcement uses to query LexisNexis databases via AFI. Criminals could then circumvent the law by developing countermeasures to the search techniques.
Exh. 3, 000034-43	Order for Supplies and Services 12/27/13	(b)(7)(E)	This document contains database-specific information identifying LexisNexis Products, the release of which would disclose law enforcement techniques and methods by which data is searched, organized and reported. This information is law enforcement sensitive information, because, when read as a whole with the rest of the Supply Order, it could reasonably allow a person to recognize identifiers that law enforcement uses to query LexisNexis databases via AFI. Criminals could then circumvent the law by developing countermeasures to the search techniques.
Exh. 3, 000044-56	Order for Supplies and Services 1/1/15	(b)(7)(E)	This document contains database-specific information identifying LexisNexis Products, the release of which would disclose law enforcement techniques and methods by which data is searched, organized and reported. This information is law enforcement sensitive information, because, when read as a whole with the rest of the Supply Order, it could reasonably allow a person to recognize identifiers that law enforcement uses to query LexisNexis databases via AFI. Criminals could then circumvent the law by developing countermeasures to the search techniques.
Exh. 3, 000057-60	Order for Supplies and	(b)(7)(E)	This document contains database-specific information identifying LexisNexis Products, the release of which would disclose law enforcement

Electronic Privacy Information Center v. U.S. Customs and Border Protection
14-1217 (RBW) (D.D.C.)
Vaughn Index for (b)(7)(E)

	Services, 9/30/09		techniques and methods by which data is searched, organized and reported. This information is law enforcement sensitive information, because, when read as a whole with the rest of the Supply Order, it could reasonably allow a person to recognize identifiers that law enforcement uses to query LexisNexis databases via AFI. Criminals could then circumvent the law by developing countermeasures to the search techniques.
--	----------------------	--	--