UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

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

NOTICE OF FILING SUPPLEMENTAL DECLARATION OF SABRINA BURROUGHS

Defendant, Customs and Border Protection ("Defendant"), through undersigned counsel, hereby submits the attached Supplemental Declaration of Sabrina Burroughs in the above captioned matter. Defendant reserves the right to further amend and/or supplement the attached declaration 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

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER	)	
Plaintiff	)	
v.	)	Civ. No.: 1:14-CV-01217-RBW
U.S. CUSTOMS AND BORDER PROTECTION	)	
Defendant.	)	

SUPPLEMENTAL DECLARATION OF SABRINA BURROUGHS

I, Sabrina Burroughs, declare as follows:

1. I am the Director of the Freedom of Information Act (FOIA) Division, Privacy and Diversity Office, Office of the Commissioner, U.S. Customs and Border Protection (CBP). As such, I am the official responsible for the overall supervision of the processing of FOIA requests submitted to CBP. I have been Director of CBP's FOIA Division in Washington, D.C., since May 20, 2013. Prior to joining CBP, I served as the Director of Disclosure Policy and FOIA Program Development for the Department of Homeland Security (DHS). As the Director of the FOIA Division, I provide technical and administrative supervision and direction, through subordinate supervisors, to a group of Government Information Specialists responsible for processing the most complex and difficult requests for release of CBP documents and information,

assist with FOIA litigation matters, and oversee the processing of FOIA responses and adherence to federal laws and regulations.

2. I am familiar with Plaintiff Electronic Privacy Information Center's (hereinafter Plaintiff) FOIA request for information from CBP that was submitted on April 8, 2014. I am also familiar with the Plaintiff's allegations in this litigation.

3. In furtherance of my responsibilities, I have access to records maintained in the ordinary course of business by CBP. All information contained herein is based upon information furnished to me in my official capacity, and the statements I make in this declaration are based on my personal knowledge, which includes knowledge acquired through, and agency files reviewed in, the course of my official duties.

4. The purpose of this declaration and the attached *Vaughn* Index is to provide additional information as to why certain information was withheld from public disclosure pursuant to 5 U.S.C. § 552(b)(7)(E), in response to the Court's order from February 17, 2016, in the above-captioned case.

5. I hereby incorporate by reference my previous declaration submitted in this case, dated May 27, 2015.

Exemption (b)(7)(E)

6. As noted above, Section 552(b)(7) of Title 5 of the U.S. Code exempts from disclosure certain records or information that are "compiled for law enforcement purposes." The records at issue in this case were compiled for law enforcement purposes in that the information is created and used by CBP in its law enforcement mission to secure the border of the United States.

7. Section 552(b)(7)(E) of Title 5 of the U.S. Code exempts from disclosure law enforcement records or information that "would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law."

8. As explained in detail in the Privacy Impact Assessment,[1] the Analytical Framework for Intelligence (AFI) system enhances DHS' ability to identify, apprehend, and prosecute individuals who pose a potential law enforcement or security risk, and aids in the enforcement of customs and immigration laws. AFI is used for the purposes of (1) identifying individuals, associations, or relationships that may pose a potential law enforcement or security risk, targeting cargo that may present a threat, and assisting intelligence product users in the field in preventing the illegal entry of people and goods; (2) conducting additional research on persons and/or cargo to understand whether there are patterns or trends that could assist in the identification of potential law enforcement or security risks; and (3) sharing finished intelligence products developed in connection with the aforementioned purposes with DHS employees who have a need to know in the performance of their official duties and who have the appropriate clearances and permissions. Finished intelligence products are tactical, operational, strategic law enforcement intelligence products that assist law enforcement agencies within DHS and also outside of DHS.

[1] Privacy Impact Assessment for the Analytical Framework for Intelligence (AFI) (Jun. 1, 2012), *available at* https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_afi_june_2012.pdf.

9. AFI augments DHS' ability to gather and develop information about persons, events and cargo of interest by creating an index of the relevant data in the existing operational systems. AFI's analytical capabilities and tools provide the link analysis between data elements and the ability to detect trends, patterns, and emerging threats. These law enforcement techniques and procedures are critical tools used by CBP officers to efficiently and effectively carry out CBP's mission to prevent terrorists, their weapons, and other dangerous items from entering the United States. The system also detects trends, patterns, and emerging threats used by law enforcement to enhance their ability to identify threats to border security.

10. Exemption (b)(7)(E) has been applied to screen shots of the AFI system and specific information regarding how to navigate and use AFI, because this information may enable an individual knowledgeable in computer systems to improperly access the system, facilitate navigation or movement through the system, allow manipulation or deletion of data and interfere with enforcement proceedings. The information regarding how to navigate and use the AFI system which has been redacted in the records provided to Plaintiff would provide a detailed roadmap to individuals looking to obtain unauthorized access to and manipulate AFI; obtain information regarding techniques used by law enforcement to identify violators and other persons of concern to law enforcement; or evade detection by law enforcement, thereby circumventing the law and potentially resulting in alteration, loss, damage or destruction of data contained in CBP's computer system.

11. Specifically, exemption (b)(7)(E) has been applied to training PowerPoints ("Modules"), AFI and Palantir Reference Cards, and documents relating to practical exercises. It has also been applied to documents detailing how to request access to AFI, how to approve access to AFI, documents relating to the operational status and security features of AFI, and a detailed document on the user roles and security access definitions. It has also been applied to several statements of work and orders for supplies and services which identify the types of data used by law enforcement officers in their efforts to identify violators and other persons of concern to law enforcement.

12. Specifically, the PowerPoint modules provide detailed, step-by-step instructions on everything from accessing AFI to how to conduct searches in AFI, including available data sources. These training modules are used to train law enforcement personnel, and, as such, the records set forth significant details regarding CBP law enforcement techniques, discussing various operational and technical aspects of the AFI system, and CBP law enforcement procedures, methods, guidance, and policies. For example, Module 1 provides an overview of AFI, including detailed tutorials, screen shots, and instructor notes designed to teach the student how to access the AFI system, how to navigate AFI and its different components and available data sources, and how to input, change, edit, and delete information in the AFI system. Further information specific to Modules 2 through 6 is provided in the attached *Vaughn* index.

13. Disclosure of the information contained in the training modules, the reference cards, and the documents relating to the practical exercises could enable

unauthorized users to gain unauthorized access to the system and alter, add, or delete information altogether, thus destroying the integrity of the system. Disclosure of this information could reasonably allow a person to recognize search terms specifically applied by law enforcement to query CBP databases. Criminals could use this information to circumvent the law by developing countermeasures aimed at defeating the effectiveness of these search techniques. Further, disclosure of this information would reveal CBP targeting and inspection techniques used in the processing of international travelers to identify persons seeking to violate U.S. law or otherwise of concern to law enforcement. Release of this information would enable potential violators to design strategies to circumvent the law enforcement techniques and measures developed by CBP.

14. Similarly, the Quick Reference Cards, the documents related to requesting, approving, and setting up AFI access, the AFI data source documents, and other documents related to the training of AFI also contain information that speak to the intricacies of the AFI system, including instructor notes regarding how to access the system, practical exercises to test the user's familiarity and proficiency with navigation and effective use of the system, and other explanations of the key elements and functionalities of the system. Public release of such law enforcement sensitive information would enable an individual knowledgeable in computer systems to improperly access the system, facilitate navigation or movement through the system, and allow for manipulation or deletion of data which would interfere with enforcement

proceedings, or permit access to information relevant to law enforcement techniques which could be used to permit circumvention of the law.

15. Exemption (b)(7)(E) has also been applied to statements of work and several orders for supplies and services. The statements of work identify database-specific information identifying LexisNexis Products employed for law enforcement purposes, the release of which would disclose 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 specific technologies and infrastructure that protect the information. Criminals could use the descriptions of the security services, critical infrastructure, and the encryption standards to bypass the security of the database and improperly access the system.

16. The orders for supplies and services contain database-specific information identifying LexisNexis Products, the release of which would disclose 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 search terms specifically applied by law enforcement to query LexisNexis databases. Criminals could then circumvent the law by developing countermeasures aimed at defeating the effectiveness of these search techniques.

17. Protecting and maintaining the integrity of CBP computer systems is imperative to CBP's ability to effectively and efficiently meet its mission to prevent terrorists, their weapons, and other dangerous items from entering the United States. As previously noted, AFI "enhances DHS's ability to identify, apprehend, and prosecute individuals who pose a potential law enforcement or security risk; and it aids in the enforcement of customs and immigration laws, and other laws enforced by DHS at the border." *See* 77 Fed. Reg. 33753, 33753 (June 7, 2012). While DHS/CBP, through its System of Records Notice[2] and Privacy Impact Assessment for AFI, have taken considerable efforts to provide the public detailed information regarding AFI, without compromising the integrity of the system, as a critical law enforcement tool employed by CBP to enhance border security, it is imperative that CBP protect AFI against any potential risk of threat or compromise to ensure CBP is able to effectively carry out its law enforcement mission.

I declare under a penalty of perjury that the information provided is true and correct to the best of my information, knowledge, and belief.

Signed this 15 day of March 2016.

Sabrina Burroughs, Director
FOIA Division
Privacy and Diversity Office
Office of the Commissioner
U.S. Customs and Border Protection
U.S. Department of Homeland Security

[2] Analytical Framework for Intelligence (AFI) System of Records, 77 Fed. Reg. 33753 (Jun. 7, 2012), *available at* https://www.gpo.gov/fdsys/pkg/FR-2012-06-07/html/2012-13813.htm.