

EXHIBIT E

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON AT SEATTLE

<hr/>	
ABDIQAFAR WAGAFE <i>et al.</i> , on behalf)
of themselves and others similarly situated,)
)
Plaintiffs,)
)
v.)
)
DONALD TRUMP, president of the)
United States <i>et al.</i> ,)
)
Defendants.)
<hr/>	

No. 17-cv-00094 RAJ

DECLARATION BY CARL (SHANE) CAMPBELL

I, Carl (Shane) Campbell hereby state as follows:

1. I am the Deputy Executive Director, Operations Directorate, Office of Field Operations (OFO), U.S. Customs and Border Protection (CBP), Department of Homeland Security (DHS). As a Deputy Executive Director for Operations, I am responsible for executing the missions of CBP and OFO. The CBP mission includes the enforcement of the customs, immigration, and agriculture laws and regulations of the United States and the enforcement of hundreds of laws at the border on behalf of numerous federal agencies. OFO is the primary CBP office responsible for securing the U.S. border at ports of entry (POEs) while facilitating lawful trade and travel. The mission of the Operations Directorate is to strengthen our borders through doctrine, comprehensive planning, direction, and resource deployments; and ensure unity of effort through information sharing, collaboration, and integration.

2. This Declaration is based on my personal knowledge, my personal review and appraisal of the claims of law enforcement privilege hereby asserted, as well as information conveyed to me by my staff and other knowledgeable CBP personnel in the course of my official duties and responsibilities.
3. I am familiar with the Motion to Compel filed by Plaintiffs on January 9, 2020 challenging law enforcement and deliberative process privilege assertions in 26 documents produced in discovery in *Wagafe v. Trump*, No. 2:17-cv-00094 (W.D. Wash.).
4. I have reviewed CBP information contained in following 21 documents:
 - 1) DEF-00000447 (Bates Begin DEF-00004010): NCTC – DS Results 3.9.12 (Final)
 - 2) DEF-00098635 (Begin Bates DEF-00052177): Vetting NS Concerns 10.02.09
 - 3) DEF-00177372 (Begin Bates DEF-00021130): CARRP Version 2.2 Aug. 2011
 - 4) DEF-01080741 (Begin Bates DEF-00044891): FDNS-DS SGN Interim SOP April 28, 2015
 - 5) DEF-01107311 (Begin Bates DEF-00017542): CARRP Processing for KSTs
 - 6) DEF-01583696 (Begin Bates DEF-00096541): DRAFT Extreme Vetting IP
 - 7) DEF-01658851 (Begin Bates DEF-00026674): FCPTC Instructor Guide
 - 8) DEF-01810149 (Begin Bates DEF-00005579): Executive Summary: CARRP Enforcement Practice Proposal (Nov. 5, 2012)
 - 9) DEF-02656545 (Begin Bates DEF-00096701): EO 13780 Updates (DRAFT)
 - 10) DEF-03206747 (Begin Bates DEF-00181890): Field Response, Gaps in CARRP
 - 11) DEF-03206769 (Begin Bates DEF-00181912): WRO Comments, CARRP Gaps
 - 12) DEF5-00173454 (Begin Bates DEF-00254790): USCIS Blue Sky Screening Ideas (Draft)

13) DEF7-00644976 (Begin Bates DEF-00261633): How the EO will Impact Vetting

14) DEF7-00789756 (Begin Bates DEF-00262350): Memo, 200-day Report, Sec. 5(b)
of EO 13780

15) DEF7-00791453 (Begin Bates DEF-00262357): DHS SCO FY2017 Goals and
Objectives (Draft)

16) DEF7-01007129 (Begin Bates DEF-00262748): Immediate Actions to Heighten
Screening and Vetting of Applications for Visas and Other Immigration Benefits
(Mar. 27, 2017)

17) DEF7-01122938 (Begin Bates DEF-00263389): EO's Impact to Vetting

18) DEF7-00644983 (Begin Bates DEF-00261640): EO's Impact to Vetting

19) DEF13-00000736 (Begin Bates DEF-00280914): CIV Business and Systems
Processes (June 20, 2018)

20) DEF-18-00000003 (Begin Bates DEF-00329157): Procedures for Identifying
CARRP Concerns

21) DEF-18-00000131 (Begin Bates DEF-00329296): NBC Job Aid, KST
Deconfliction.

5. Further, I reviewed CBP information in the following 5 documents from the Certified
Administrative Record (CAR):

a. DEF-00095009, Operational Guidance for Vetting and Adjudicating Cases with
National Security Concerns

b. DEF-00116759, FDNS National Security Division, Controlled Application Review
and Resolution Program (CARRP), Updated June 2017

- c. DEF-00132598, Fact Sheet, Frequently Asked Questions CARRP Policy and Operational Guidance
 - d. DEF-00277275, USCIS Handbook, National Background Identity and Security Checks Operating Procedures, December 17, 2010
 - e. DEF-00373850, FDNS National Security Division, Controlled Application Review and Resolution Program (CARRP), Updated December 2015
6. I have personally reviewed the CBP information that was withheld from production in the 21 documents listed above in addition to 5 documents from the CAR. Information in the above-listed documents falls in the following three categories:
 - a. Computer codes and screenshots from CBP systems
 - b. Information related to law enforcement vetting and screening
 - c. Information related to specific law enforcement methods, techniques and procedures designed to identify national security threats
7. I have reviewed the declaration by Deputy Assistant Executive Commissioner for OFO, Mr. John P. Wagner filed with the court on April 26, 2019 (hereinafter, Wagner Declaration), asserting law enforcement privilege over CBP information in a set of documents subject to Plaintiff's April 11, 2019 Motion to Compel. *See* Attachment. I agree with the statements made in the Wagner Declaration regarding the sensitivity of CBP records, particularly in paragraphs 10 through 20. I believe that the statements in paragraphs 10 through 20 of the Wagner Declaration apply to the three categories of CBP information in the 26 documents listed above.
8. The disclosure of CBP information in the above-listed 26 documents would be contrary to the public interest, because it would reveal information about CBP's law enforcement

- methods, techniques, and practices, identify and expose sensitive information about CBP's law enforcement systems, and disclose information about CBP's law enforcement vetting.
9. This disclosure would impact CBP's ability to conduct its enforcement operations, allow potential violators to discover or circumvent CBP investigative techniques, and endanger CBP operations and personnel at POEs. For the reasons set forth in paragraphs 10 through 20 of the Wagner Declaration, the disclosure of this information would enable potential violators to evade CBP inspection processes and law enforcement activities, and threaten border security, national security, and the safety of CBP Officers and the public. The disclosure of the withheld information would also jeopardize the overall effectiveness of interagency communication.
10. Therefore, I respectfully assert the law enforcement privilege over CBP information in the 26 documents listed above, as well as for any other document relevant in discovery for the above-captioned case that contains computer codes and screenshots from CBP Systems, CBP information related to law enforcement screening and vetting, and CBP information related to specific law enforcement methods, techniques and procedures designed to identify national security threats.

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

Executed on the 4th day of February, 2020



Carl (Shane) Campbell
Deputy Executive Director, Operations
Office of Field Operations
U.S. Customs and Border Protection

EXHIBIT E-1

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON AT SEATTLE

ABDIQAFAR WAGAFE *et al.*, on behalf)
of themselves and others similarly situated,)
))
Plaintiffs,)
))
v.)
))
DONALD TRUMP, president of the)
United States *et al.*,)
))
Defendants.)

No. 17-cv-00094 RAJ

DECLARATION ASSERTING LAW ENFORCEMENT PRIVILEGE

I, John P. Wagner, hereby state as follows:

1. I am the Deputy Executive Assistant Commissioner, Office of Field Operations (OFO), U.S. Customs and Border Protection (CBP), Department of Homeland Security (DHS). I have been employed in this role since April 16, 2014. I began my career with the U.S. Customs Service as a Customs Inspector in 1991, and I had several assignments in the field, including at the New York/New Jersey seaport and the Laredo port of entry. I was also detailed to the Department of Homeland Security, Border and Transportation Security Directorate. I have been assigned to the Office of Field Operations at Headquarters since 1999. I have worked on many different policy and operational issues during my time at headquarters, including serving as Executive Director, Admissibility and Passenger Programs.
2. In my role as the Deputy Executive Assistant Commissioner, I am responsible for executing the missions of CBP and OFO. The CBP mission includes the enforcement of the customs, immigration, and agriculture laws and regulations of the United States and

the enforcement of hundreds of laws at the border on behalf of numerous federal agencies. OFO is the primary CBP office responsible for securing the U.S. border at ports of entry (POEs) while facilitating lawful trade and travel. In my position, I supervise more than 28,000 employees, with operations at 20 major field offices, 328 POEs, and 70 locations in over 40 countries internationally.

3. As Deputy Executive Assistant Commissioner, I am familiar with CBP's administration and enforcement of legal requirements at the border, including the enforcement and administration of immigration laws, the inspection, processing, and admission of persons who seek to enter or depart the United States, and the detection, interdiction, removal, departure from the United States, short-term detention, and transfer of persons unlawfully entering, or who have recently unlawfully entered, the United States. To accomplish its mission, CBP officers conduct searches and inspections at the border and its functional equivalent. This requires using a variety of investigative and law enforcement techniques to determine, among other things, whether an alien is admissible to the United States. It also entails the exercise of border search authority, which authorizes CBP officers to detain and search persons and property at the border without suspicion or a warrant.
4. The effectiveness of CBP's mission is dependent to a large extent on the use of sensitive investigative techniques and methods that are not known to the general public. The disclosure of these techniques and methods would seriously compromise CBP's ability to perform its law enforcement mission to enforce the law at the border.
5. This declaration is based on my personal knowledge, my personal review and appraisal of the claims of law enforcement privilege hereby asserted and the factual background of the

case, as well as information conveyed to me by my staff and other knowledgeable CBP personnel in the course of my official duties and responsibilities.

6. I am aware of the Motion to Compel filed by Plaintiffs on April 11, 2019, challenging the assertion of law enforcement and deliberative process privilege over 25 documents produced in discovery in *Wagafe v. Trump*, No. 2:17-cv-00094 (W.D. Wash.).
7. I am making this declaration for the purpose of asserting the law enforcement privilege over CBP information that is contained in, and has been redacted from the following 23¹ documents:
 - a. Policy Memorandum 602-XXXX [DEF-0094235-DEF-0094252];
 - b. Operational Guidance for Vetting and Adjudicating Cases with National Security Concerns [DEF-00095009-DEF-00095054];
 - c. Additional Guidance on Issues Concerning the Vetting and Adjudication of Cases Involving National Security Concerns [DEF-0094260- DEF-0094268];
 - d. Senior Policy Council - Briefing Paper [DEF-0094275-DEF-0094277];
 - e. CARRP Adjudicator Training - Instructor Guide [DEF-0094295-DEF-0094348];
 - f. Refugee Adjudication Standard Operating Procedure: Cases Involving National Security Concerns [DEF-00095055-DEF-00095076];
 - g. National Security Indicator Training, January 2017 [DEF-0094351-DEF-0094535];
 - h. CARRP Operational Guidance: Attachment A - Guidance for Identifying National Security Concerns [DEF-0094536-DEF-0094544];
 - i. Operational Guidance for Vetting and Adjudicating Cases with National Security Concerns [DEF-00095077-DEF-00095122];

¹ Two documents listed in Plaintiff's motion to compel "Executive Summary RE: Controlled Application Review and Resolution Program (CARRP), Redesignated as the Situational Review Process (SRP)," January 6, 2017 [DEF-0094269-DEF-0094270]" and "Case Prioritization Intelligence Assessment (CPIA) [DEF-0094271-DEF-0094274]" do not contain any CBP law enforcement sensitive information, and thus this declaration only applies to 23 documents that contain CBP information.

- j. CARRP Overview - Refugee Asylum, and International Operations Directorate (RAIO) Pre-Deployment Training [DEF-0094545-DEF-0094629];
 - k. National Security Indicator Training, August 2017 [DEF-0094630-DEF-0094792];
 - l. [Redacted]: Where do They Come From and Where do They Go? [DEF-00095123];
 - m. Where do [Redacted] Come From? [DEF-00095124];
 - n. National Security Indicator Training, August 2017 [DEF-00095125-DEF-00095285];
 - o. National Security Indicator Training, August 2017 [DEF-0094804-DEF-0094966];
 - p. CARRP Policy/Guidance Questions [DEF-0094974-DEF-0094978];
 - q. National Security Indicator Training, August 2017 [DEF-00095597-DEF-00095757];
 - r. USCIS Shark Tank [DEF-0094994-DEF-0095008];
 - s. FDNS Officer Basic Training: National Security Instructor Guide [DEF-00095760-DEF-00095870];
 - t. FDNS Officer Basic Training: Identification of a NS Concern [DEF-00095871-DEF-00095962];
 - u. FDNS Data System (“FDNS-DS”) User Guide Updates & Articulate Link Training [DEF-00095963-DEF-00096057];
 - v. Interim Operational Guidance Pertaining to the Vetting and Adjudication of Cases with National Security Concerns [DEF-00096058-DEF-00096100];
 - w. FDNS Continuous Immigration Vetting (CIV) Overview [DEF-00096101-DEF-00096104]
8. I have personally reviewed the CBP information that was withheld from production in the 23 documents listed above. For the reasons set forth below, I have determined that the disclosure of this information would be contrary to the public interest, because it would reveal information about CBP’s law enforcement methods, techniques, and practices,

identify and expose sensitive information about CBP's law enforcement systems, and disclose information about CBP's law enforcement vetting.

9. CBP information contained in the 23 documents listed above falls into the following categories:
 - a. Computer codes and screenshots from CBP systems
 - b. Information related to law enforcement vetting and screening
 - c. Information related to specific law enforcement methods, techniques and procedures designed to identify national security threats

A. Computer Codes and Screenshots

10. TECS, which is principally owned and managed by CBP, is an overarching law enforcement information collection, analysis, and sharing environment that securely links telecommunications devices and personal computers to a central system and database. This environment is comprised of several modules designed to collect, maintain, and vet data as well as conduct analysis, risk assessments, and information sharing. TECS contains temporary and permanent enforcement, inspection, and intelligence records relevant to the law enforcement mission of CBP and numerous other federal agencies that it supports. TECS is CBP's principal law enforcement and anti-terrorism data base system. TECS is described in further detail in the Federal Register at 73 Fed. Reg. 77778 (Dec. 19, 2008). TECS contains law enforcement sensitive data, and access to TECS is tightly constrained, even within CBP.
11. The documents (a) through (w) listed at paragraph 7 above, contain TECS computer codes and provide additional context to explain the meaning and relevance of certain TECS codes. Individuals who know the meaning of TECS codes would have sufficient law

enforcement information regarding how CBP conducts its law enforcement operations, which would permit individuals to alter their patterns of conduct, adopt new methods of operation, relocate, change associations, and effectuate other countermeasures, thus corrupting the integrity of ongoing law enforcement operations. Revealing information explaining TECS codes to the public would disclose to individuals the nature of the government's interest in them, reveal subjects of government investigations, and jeopardize and impair such investigations. Further, illicit actors who are provided such information could learn how CBP communicates law enforcement sensitive information internally within its systems and find out whether they are subject to any investigations and inquiries. This would allow such illicit actors to change behavior and tactics to avoid detection.

12. Revealing the TECS screenshots in the documents listed at paragraph would reveal additional codes and could facilitate access to, and navigation through, TECS. Public dissemination of these access codes would reveal the technical capabilities of the system and if the system were improperly accessed, could permit unauthorized users to manipulate records, including manipulating the way certain records are created and maintained, to avoid recognition, detection and apprehension. It would also arm unauthorized users with the ability to corrupt the integrity of the data contained therein through the alteration/manipulation of such data. Therefore, disclosure of these codes could put at risk ongoing investigations and border security operations.

13. In addition to system codes, screenshots from CBP systems, such as TECS, are sensitive as the interface of the sensitive government database reveals how law enforcement information is presented and communicated to officers. If such information were to be

available to public, bad actors could reverse engineer CBP systems, or manipulate information available to officers during inspection. Although a few factors considered by CBP officers when conducting border searches are in the public domain in court opinions and other contexts, the TECS format itself reveals more about the techniques that CBP officers use to process travelers and assess risk than can be gleaned from information currently available to the public. Because the data fields for entering information in TECS are of limited capacity, information entered into the data fields must necessarily be abbreviated. Disclosure of this shorthand communication would serve no legitimate public interest as its meaning would be irretrievably distorted once taken from the tightly controlled context in which it is created, interpreted and shared by and between trained law enforcement personnel.

14. Further, information in TECS screenshots reveal the search capabilities of TECS, release of which would impede CBP's law enforcement mission by alerting individuals to how CBP conducts searches of its systems and any limitations of the search capabilities. Disclosure of this information would reveal possible gaps that may be exploited by illicit actors to avoid detection.
15. TECS also includes information originating with third agencies or departments. Disclosure of such information, as contained in documents listed in paragraph 7, threatens efforts to foster open communication across agencies and cohesive law enforcement and national security efforts. Disclosure of the information contained in these records could have far-reaching effects, impairing other agencies' law enforcement operations or their ability to effectively carry out their respective missions. Knowledge of this information would

increase the risk of circumvention of laws and regulations, impede effectiveness of law enforcement activities, and endanger agency investigative practices and techniques.

B. Information Regarding Law Enforcement Vetting and Targeting Activities

16. The Automated Targeting System (ATS) is a decision support tool that compares traveler, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data using risk-based targeting scenarios and assessments. The Department of Homeland Security (DHS)/CBP operates ATS to facilitate legitimate trade and travel while managing the shared threat to the homeland posed by certain people or cargo entering or exiting the United States. ATS supports CBP in identifying individuals and cargo that may require additional scrutiny across various transportation networks using various functionalities.² CBP has made information about ATS publicly available at <https://www.dhs.gov/publication/automated-targeting-system-ats-update/>.

17. Documents DEF-00096101, DEF-00096058, DEF-00095871, contain sensitive information related to CBP's vetting and targeting operations. Specifically, these documents reveal types of information CBP considers when vetting individuals against law enforcement data and CBP's priorities when it analyzes such information. Disclosure of these records would reveal law enforcement privileged information about vetting activities generally, such as the kind of information CBP considers and evaluates and the categories of information communicated to officers to inform their discretion, and the relative importance given different factors. Information about such lines of indicators if

² Automated Targeting System, Privacy Impact Assessment, DHS/CBP/PIA-006(d), <https://www.dhs.gov/publication/automated-targeting-system-ats-update>.

unprotected, can enable individuals to thwart efforts to secure the border and enforce customs and immigration laws.

18. In addition, these three documents described in paragraph 17 contain specific descriptions and uses of different types of “lookouts” generated by CBP based on information available in its systems, types of information CBP considers to generate the lookouts, as well as codes and data fields used to communicate such lookouts to CBP officers in the field and other government agencies. The release of specific information related to lookouts would have the unintended and undesirable effect of placing CBP’s law enforcement techniques and strategies in the public domain and at the disposal of potentially illicit actors; educating them as to the investigative techniques used and thereby assisting them to devise methods to evade detection and apprehension; and, ultimately, impairing the effectiveness of those law enforcement techniques.

19. Information that CBP considers when vetting individuals is particularly sensitive because understanding what information CBP analyzes and prioritizes when conducting vetting would allow individuals to identify any possible gaps, manipulate information provided to CBP, change behavior and avoid detection.

C. Law Enforcement Methods, Techniques and Procedures To Identify National Security Threats

18. Documents DEF-00096058, DEF-00095871, and DEF-00095760 contain information related to CBP methods, techniques, and procedures designed to identify national security threats. Information describing specific methods, techniques, and procedures is highly sensitive and identify CBP’s highest priorities for targeting high-risk travelers that threaten border security and national security. Releasing such information would reveal how CBP connects various pieces of information about existing national security threats to use in

creating targeting criteria to identify future high-risk travelers. Disclosure of such information would thwart CBP's efforts to identify national security threats and would alert individuals that they may be of national security or law enforcement interest. Such information, if unprotected, could enable individuals to thwart CBP's efforts to secure the border and enforce various laws, including customs and immigration laws. Disclosure of this information would identify law enforcement priorities and conversely, areas where investigative resources may not be focused. If revealed, that information could be exploited and used to develop and employ more effective counter-measures to diminish the effectiveness of inspection efforts. Accordingly, such information is protected by the law enforcement privilege.

CONCLUSION

20. In my judgment, the disclosure of CBP law enforcement privileged information contained in and redacted from the 23 documents discussed herein, and listed in paragraph 7, would allow potential violators to discover or circumvent CBP investigative techniques, and endanger CBP operations and personnel at POEs. Specifically, the disclosure of this information would enable potential violators to evade CBP inspection processes and law enforcement activities, and threaten border security, national security, and the safety of CBP Officers and the public. The disclosure of the withheld information would also jeopardize the overall effectiveness of interagency communication.
21. Accordingly, in my opinion, disclosure of CBP information in the 23 documents would impede law enforcement and impair CBP's ability to apprehend violators of the laws enforced by CBP.

22. Therefore, I respectfully assert the law enforcement privilege over CBP information in the 23 documents described above, for the reasons set forth above.

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

Executed on the 25 day of APRIL, 2019



John P. Wagner
Deputy Executive Assistant Commissioner
Office of Field Operations
U.S. Customs and Border Protection