**UNITED STATES DISTRICT COURT**
**EASTERN DISTRICT OF VIRGINIA**
**ALEXANDRIA DIVISION**

| | | |
|---|---|---|
| GULET MOHAMED, | ) | |
| Plaintiff, | ) | |
| v. | ) | Case No. 1:11-CV-0050 |
| ERIC H. HOLDER, JR., in his official capacity as Attorney General of the United States, *et al*., | ) | |
| Defendants. | ) | |

**DEFENDANTS' MEMORANDUM OF LAW IN OPPOSITION TO PLAINTIFF'S MOTION TO COMPEL**

Pursuant to Local Rule 7(F)(1) and this Court's Rule 16(B) Scheduling Order, Defendants, through their undersigned counsel, hereby respectfully submit this opposition to Plaintiff's motion to compel Defendants' response to interrogatories and requests for production. ECF No. 91 ("Motion").

## TABLE OF CONTENTS

## INTRODUCTION

Plaintiff seeks the production of highly sensitive national security and law enforcement information that is protected from disclosure by privilege. In this suit, he challenges his alleged placement on the No Fly List, a subset of the Terrorist Screening Database ("TSDB"), and seeks prospective injunctive relief removing him from the No Fly List and related databases. Defendants, the Terrorist Screening Center ("TSC") and the Federal Bureau of Investigation ("FBI"), have made reasonable discovery responses.[1] Ultimately, however, Plaintiff's discovery requests seek information that is sensitive and rooted in this nation's counterterrorism efforts. Defendants have agreed to produce unprivileged and unclassified documents and information detailing the policies and procedures governing the No Fly List, final reviews and audits of the TSDB, and statistics about the TSDB, Selectee List, and No Fly List; but the parties were nonetheless unable to reach agreement on the proper scope of discovery and the applicability of privileges.

Plaintiff's challenge to his alleged placement on the No Fly List hinges on highly sensitive national security and law enforcement information that is properly protected from disclosure under the law, including: (1) information that could tend to reveal whether or not the Plaintiff has been the subject of an investigation, including the contents of any relevant counterterrorism investigative files, to the extent they exist; (2) information that could tend to reveal the basis, nature, status, or results of any FBI counterterrorism investigation or intelligence operation; and (3) information that could tend to reveal whether particular sources

[1] Plaintiff's Fourth Amended Complaint added the Department of Homeland Security ("DHS") and the Transportation Security Administration ("TSA") as defendants. *See* ECF No. 84 (order), 85 (complaint). Plaintiff has not served requests for discovery on DHS or TSA, and if such discovery is served, TSA and DHS would provide appropriate responses, which could include additional objections that were not asserted by either TSC or FBI.

and methods were used by the FBI in any counterterrorism investigation or intelligence operation (if any) of Plaintiff, his associates, or others. This information, which is sought in discovery and/or relevant to the claims and defenses in this matter, is properly protected by the state secrets privilege. As explained in the declaration of Attorney General Eric H. Holder, Jr., as well as the supporting FBI classified declaration submitted to the Court for its *ex parte* and *in camera* review, disclosure of the information Plaintiff seeks reasonably could be expected to cause significant harm to national security. As a result, the Attorney General has asserted the state secrets privilege over this information, and based on this privilege assertion, Defendants have separately moved for dismissal. Discovery should not proceed until that motion is resolved.

In addition, Plaintiff's discovery requests implicate a number of other types of privileged information, including law enforcement sensitive information and Sensitive Security Information ("SSI," which is protected from disclosure by statute). Much of this information is irrelevant to Plaintiff's claims, including information that predates any of the alleged events in this case, information about individuals other than Plaintiff, and information that cannot be readily or reliably obtained from the TSDB. The burden involved in attempting to assemble this information far outweighs any arguable relevance to the matter at hand, and in any event, much of the information is protected by the law enforcement privilege, as established by the separate classified declaration of John Giacalone, Assistant Director of the FBI's Counterterrorism Division, which is also submitted to the Court for its *ex parte* and *in camera* review. Plaintiff's Motion should therefore be denied.

## BACKGROUND

Plaintiff is a naturalized U.S. citizen who was denied boarding on one flight returning to the United States in early 2011, but was able to return on a different flight a few days later. ECF

No. 85 ("Fourth Am. Compl.") ¶¶ 7, 51-52. His Fourth Amended Complaint purports to make three claims: a "right to citizenship" claim based on denial of his alleged right to return to the United States (essentially a substantive due process claim, as discussed below); a procedural due process claim; and an Administrative Procedure Act claim. *See generally id*. This Court, however, has already partly dismissed Plaintiff's "citizenship" claim, finding that his "own allegations establish that … he was able to board a flight on January 20, 2011 and reenter the United States without incident on January 21, 2011." *See* ECF No. 70 ("Mem. Op.") at 27; ECF No. 71 (order dismissing in part). The Court held that such a delay did not amount to a constitutional deprivation. Mem. Op. at 27; *see also* ECF No. 92 (order denying Plaintiff's motion to reconsider dismissal of the return claim). In the same ruling, the Court allowed Plaintiff to proceed with his substantive and procedural due process claims, namely: (1) whether the disabilities he alleges flow from his alleged inclusion on the No Fly List unconstitutionally burden "the exercise of his right of exit and reentry;" and (2) whether "DHS TRIP provides sufficient process to defeat" Plaintiff's procedural due process claim." Mem. Op. at 27-31. Finally, the Court found that Plaintiff's APA claim "essentially conflate[s] with his constitutional claims." *Id.* at 31.

On February 19, 2014, Plaintiff served discovery requests on the FBI and TSC that sought a wide array of information about watchlisting dating to 2003. *See* Pl's 1st Set of Requests for Production, ECF No. 91 (Motion Exh. A-1) ("RFPs"); Pl's 1st Set of Interrogatories (Motion Exh. A) ("Interrogatories"). The parties conferred, and Defendants responded to the requests for discovery (Motion Exhs. B & B-1). Since that time, Defendants have produced approximately 500 pages of documents. Defendants have also created a privilege log for withheld documents, and, as set forth herein, the privileged information being withheld is

properly protected by law. Defendants have also lodged classified and/or law enforcement sensitive declarations in support of their assertions of privileges in response to Plaintiff's discovery requests.[2]

**ARGUMENT**

**I. The State Secrets Privilege**

Plaintiff's Motion seeks the production of classified and otherwise privileged national security information that is subject to withholding under the state secrets privilege. For example, Plaintiff seeks documents or information concerning: (1) the basis for an individual's placement or alleged placement in the TSDB (*e.g.*, RFP 8 (seeking documents "regarding the inclusions of U.S. citizens in the No-Fly List while they are abroad"), RFP 9 (seeking documents "concerning TSC's processing of Traveler Redress Inquiry Program (TRIP) complaints from person placed in the No-Fly List, Selectee List, or TSDB"), RFP 11 (seeking documents regarding Plaintiff); Interrogatory 10 ("For the years 2003 to the present, as to each U.S. citizen who has been removed from the TSDB, Selectee List, or the No-Fly List, or whose placement thereon has been changed from one list to another, list specific reasons for said removal or change.")); and (2)

[2] Defendants' privilege log must be lodged for *ex parte* and *in camera* review in order to avoid disclosing information to Plaintiff that would reveal the very privileged information Defendants are trying to protect. *See* Fed. R. Civ. P. 26(b)(5)(ii) (requiring party to describe the nature of the documents, communications, or tangible things not produced or disclosed," but that a party need not do so by "revealing information itself privileged or protected."); *United States v. Abu Ali*, 528 F.3d 210, 245 (4th Cir. 2008) ("validity of [evidentiary] privileges may be tested by *in camera* and *ex parte* proceedings before the court for the limited purpose of determining whether the asserted privilege is genuinely applicable.") (internal quotation marks omitted). These principles apply with equal force to the provision of privilege logs, where the submission of details associated with privileged documents could itself reveal privileged information. *See Bassiouni v. CIA*, 392 F.3d 244, 246-47 (7th Cir. 2004) (agency may acknowledge the existence of responsive documents but withhold information about the number or volume of responsive documents or their content, where such descriptive information is itself, or would tend to reveal, classified or otherwise protected information); *see also CIA v. Sims*, 471 U.S. 159, 179 (1985) ("It is conceivable that the mere explanation of why information must be withheld can convey valuable information to a foreign intelligence agency.").

watchlisting policies and procedures (*e.g.*, RFP 1 (seeking "documents regarding policy standards and procedural and substantive rules used to determine inclusion on the No-Fly List.")).

As set forth herein and in the accompanying declarations, disclosure of such information in this litigation reasonably could be expected to cause significant harm to national security. Accordingly, the Attorney General of the United States has now formally asserted the state secrets privilege to protect that information from disclosure. Because the privilege has been properly invoked and supported, the Court should uphold the state secrets privilege assertion, deny Plaintiff's motion to compel with respect to the information over which the Government has asserted this privilege, and, for the reasons set forth in Defendants' simultaneously-filed dispositive motion, dismiss Plaintiff's lawsuit.

### A. The State Secrets Privilege Protects Against Disclosure of Information That Reasonably Could Be Expected to Harm National Security.

The Supreme Court has long recognized the Government's ability to protect state secrets from disclosure in litigation. *See United States v. Reynolds*, 345 U.S. 1, 7–8 (1953) (discussing *Totten v. United States*, 92 U.S. 105 (1875)); *Gen. Dynamics Corp. v. United States*, 131 S. Ct. 1900 (2011) ("We have recognized the sometimes-compelling necessity of governmental secrecy by acknowledging a Government privilege against court-ordered disclosure of state and military secrets."); *El-Masri v. United States*, 479 F.3d 296, 304 (4th Cir. 2007). The privilege to protect state secrets derives from the President's Article II authority over foreign affairs and national defense matters. *See United States v. Nixon*, 418 U.S. 683, 710 (1974); *see also El-Masri*, 479 F.2d at 303–304 (noting "constitutional dimension" of privilege). For these reasons, as one court has observed, the privilege to protect state secrets "must head the list" of various privileges recognized in courts. *See Halkin v. Helms*, 598 F.2d 1, 7 (D.C. Cir. 1978) ("*Halkin I*"); *see also*

*El-Masri v. Tenet*, 437 F. Supp. 2d 530, 536 (E.D. Va. 2006) (privilege to protect state secrets is "of the highest dignity and significance"), *aff'd*, 479 F.3d 296 (4th Cir. 2007).

As relevant here, the state secrets privilege is an evidentiary privilege that excludes privileged evidence from a case.[3] *El-Masri*, 479 F.3d at 303; *Mohamed v. Jeppesen Dataplan, Inc*, 614 F.3d 1070, 1077 (9th Cir. 2010) (en banc) (citing *Reynolds*). Analyzing a state secrets privilege claim under the *Reynolds* doctrine involves three steps. First, a court must determine that the procedural requirements for invoking the state secrets privilege have been satisfied, in particular, whether the head of the department or agency responsible for the evidence at issue has personally considered the need to protect the information and formally asserted privilege. *See El-Masri*, 479 F.3d at 304. Second, a court must decide whether the evidence the Government seeks to protect qualifies as privileged under the state secrets doctrine and should thus be excluded. *See id.* In making this determination, courts may assess only whether there is a "reasonable danger" that disclosure would harm national security, and must give the "utmost deference" to the Government's judgment on the risk of harm to national security. *See id.* at 305. Third, if the privilege assertion is upheld, a court must assess whether the excluded evidence is so central to the litigation that dismissal is required, or whether the case can proceed in the ordinary course without the privileged information. *Id*. at 306-08. Defendants will address each of these requirements in turn.

[3] Courts have recognized this as one of two overarching applications of the state secrets privilege doctrine. Another application (not raised in this case) based on the Supreme Court's 1875 decision in *Totten v. United States*, 92 U.S. 105 (1875), permits dismissal where it is apparent that the very subject matter of the action will require the disclosure of state secrets that would result in harm to national security. *See Jeppesen*, 614 F.3d at 1077-78 (discussing the "*Totten* bar"); *see also Gen. Dynamics*, 131 S. Ct. at 1906–07; *Tenet v. Doe*, 544 U.S. 1, 8–10 (2005).

### 1. Procedural Requirements for Privilege Assertion

First, as a procedural matter, "[t]he privilege belongs to the Government and must be asserted by it; it can neither be claimed nor waived by a private party." *Reynolds*, 345 U.S. at 7. *Reynolds* emphasized that the state secrets privilege "is not to be lightly invoked," and several procedural constraints on its assertion "give practical effect to that principle." *El-Masri*, 479 F.3d at 304. Specifically, to invoke the privilege: (1) there must be a "formal claim of privilege"; (2) the claim must be "lodged by the head of the department which has control over the matter"; and (3) the claim must be made "after actual personal consideration by that officer." *Reynolds*, 435 U.S. at 7–8. Accordingly, an assertion of the state secrets privilege is no ordinary or simple occurrence; rather, it constitutes a judgment at the highest levels of the Executive Branch that the disclosure of privileged information reasonably could be expected to harm national security.

### 2. Judicial Review of the Privilege Assertion

After a court has confirmed that the procedural prerequisites for asserting the privilege are satisfied, it must determine whether the information that the United States seeks to shield is privileged from disclosure. *See El-Masri*, 479 F.3d at 304. The standard of review governing an invocation of the state secrets privilege is highly deferential. As set forth in *Reynolds*, the court must assess whether, under the particular circumstances of the case, "there is a reasonable danger that compulsion of the evidence will expose military matters which, in the interest of national security, should not be divulged." *Reynolds*, 345 U.S. at 10.[4] Under this standard, courts give

[4] The law is clear that the privilege encompasses a range of information broader than military matters, to include information that would result in "impairment of the nation's defense capabilities, disclosure of intelligence-gathering materials or capabilities, and disruption of diplomatic relations with foreign governments." *Ellsberg v. Mitchell*, 709 F.2d 51, 57 (D.C. Cir. 1983); *accord Gen. Dynamics*, 131 S. Ct. at 1905 ("Protecting our national security sometimes

"utmost deference" to the Government's judgment as to whether a disclosure would risk harm to national security. *See Nixon*, 418 U.S. at 710 (discussing privilege for military or diplomatic secrets and recognizing that courts have traditionally shown "utmost deference" to these areas of Article II duties); *El-Masri*, 479 F.3d at 305 (recognizing "utmost deference" standard); *Kasza*, 133 F.3d at 1166 (same); *Zuckerbraun v. Gen. Dynamics Corp.*, 935 F.2d 544, 547 (2d Cir. 1991) (same); *see also Al-Haramain Islamic Found., Inc. v. Bush*, 507 F.3d 1190, 1203 (9th Cir. 2007) (observing that, in evaluating the need for secrecy, courts must "acknowledge the need to defer to the Executive on matters of foreign policy and national security and surely cannot legitimately find ourselves second guessing the Executive in this arena.").

In adjudicating a state secrets claim, the court does not balance the respective needs of the parties for the information. Rather, once the privilege is properly invoked and the court is satisfied that there is a reasonable danger that national security would be harmed by the disclosure of state secrets, the privilege is absolute. "Where there is a strong showing of necessity, the claim of privilege should not be lightly accepted, but even the most compelling necessity cannot overcome the claim of privilege if the court is ultimately satisfied that military secrets are at stake." *Reynolds*, 345 U.S. at 11; *El-Masri*, 479 F.3d at 304; *Zuckerbraun*, 935 F.2d at 547; *Kasza*, 133 F.3d at 1166; *see also In re Under Seal*, 945 F.2d 1285, 1287 n.2 (4th Cir. 1991) (state secrets privilege "renders the information unavailable regardless of the other party's need in furtherance of the action").[5]

---

requires keeping information about our military, intelligence, and diplomatic efforts secret."); *see also Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998).

[5] *See also Northrop Corp. v. McDonnell Douglas Corp.*, 751F.2d 395, 399 (D.C. Cir. 1984) (state secrets privilege "cannot be compromised by any showing of need on the part of the party seeking the information"); *Ellsberg*, 709 F.2d at 57 ("When properly invoked, the state secrets privilege is absolute. No competing public or private interest can be advanced to compel disclosure of information found to be protected by a claim of privilege.").

The absolute nature of the state secrets privilege applies to exclude the evidence regardless of the nature or significance of the claim at issue, including where constitutional claims are at stake. *See El-Masri*, 479 F.3d at 311-12 (state secrets protected in constitutional tort challenge to alleged unlawful rendition by CIA); *Halkin I, supra*; *Halkin v. Helms*, 690 F.2d 977 (D.C. Cir. 1982) ("*Halkin II*") (state secrets protected in constitutional challenge to alleged unlawful surveillance); *Molerio v. FBI*, 749 F.2d 815 (D.C. Cir. 1984) (state secrets protected where First Amendment associational rights at issue). The court may consider the necessity of the information to the case only in connection with assessing the sufficiency of the Government's showing that there is a reasonable danger that disclosure of the information at issue would harm national security. "[T]he more plausible and substantial the government's allegations of danger to national security, in the context of all the circumstances surrounding the case, the more deferential should be the judge's inquiry into the foundations and scope of the claim." *Ellsberg*, 709 F.2d at 59.

Consequently, classified declarations may be submitted for *ex parte, in camera* review in cases where the state secrets privilege is invoked. *El-Masri*, 479 F.3d 29, 30; *Fitzgerald v. Penthouse Int'l, Ltd.*, 776 F.2d 1236 (4th Cir. 1985); *Molerio*, 749 F.2d at 819, 822; *Farnsworth Cannon, Inc. v. Grimes*, 635 F.2d 268, 281 (4th Cir. 1980) (*en banc*).[6]

[6] *See, e.g.*, *In re United States*, 872 F.2d 472, 474 (D.C. Cir. 1989) (classified declaration of assistant director of the FBI's Intelligence Division submitted for *in camera* review in support of Attorney General's formal invocation of state secrets privilege); *Fazaga v. FBI*, 884 F. Supp. 2d 1022, 1030 (C.D. Cal. 2012) (Government submission of *ex parte, in camera* declarations to support privilege); *Al-Aulaqi v. Obama*, 727 F. Supp. 2d 1, 53 n.15 (D.D.C. 2010) (same); *Tilden v. Tenet*, 140 F. Supp. 2d 623, 626–27 (E.D. Va. 2000) (same). The examination of *ex parte* material is not, however, required when the Court can decide the question on the basis of unclassified material. *See Reynolds*, 345 U.S. at 8-10 ("we will not go so far as to say that the court may automatically require a complete disclosure to the judge before the claim of privilege will be accepted in any case" and where the court can determine that the "occasion for the privilege is appropriate . . . the court should not jeopardize the security which the privilege is

### 3. Impact of the Exclusion of Privileged Evidence

"If the subject information is determined to be privileged [as a result of the invocation of the state secrets privilege], the ultimate question to be resolved is how the matter should proceed in light of the successful privilege claim. *El-Masri*, 479 F.3d at 304. The court's determination that "a piece of evidence is a privileged state secret removes it from the proceedings entirely," *Id.* at 306. What this exclusion means for a particular litigation "will vary from case to case." *Id.* (quoting *Sterling*, 416 F.3d at 348); *Fitzgerald*, 776 F.2d at 1243-44. In some cases, after the privileged evidence is excluded, "the case will proceed accordingly, with no consequences save those resulting from the loss of evidence."' *Al-Haramain*, 507 F.3d at 1204 (quoting *Ellsberg*, 709 F.2d at 64). But the law is clear that dismissal is required where state secrets are inextricably bound up in any consideration of the merits. *Gen. Dynamics Corp.*, 131 S. Ct. at 1903-1906; *El-Masri*, 479 F.3d at 308 ("[A] proceeding in which the state secrets privilege is successfully interposed must be dismissed if the circumstances make clear that privileged information will be so central to the litigation that any attempt to proceed will threaten that information's disclosure."); *Fitzgerald*, 776 F.2d at 1241–42 ("[I]n some circumstances sensitive military secrets will be so central to the subject matter of the litigation that any attempt to proceed will threaten disclosure of the privileged matters."). The requirements for dismissal are discussed in more detail in Defendants' separately filed memorandum in support of their motion to dismiss the Complaint.

### 4. Attorney General's Policy

In addition to the foregoing requirements in established case law, on September 23, 2009, the Attorney General announced a new Executive branch policy governing the assertion and

---

meant to protect by insisting upon an examination of the evidence, even by the judge alone, in chambers.").

defense of the state secrets privilege in litigation. Under this policy, the U.S. Department of Justice will defend an assertion of the state secrets privilege, and seek dismissal of a claim on that basis, "only when doing so is necessary to protect against the risk of significant harm to national security." *See* Exhibit 1 to Holder Declaration (State Secrets Policy); *see also Jeppesen*, 614 F.3d at 1077 (discussing Policy). Moreover, "[t]he Department will not defend an invocation of the privilege in order to: (i) conceal violations of the law, inefficiency, or administrative error; (ii) prevent embarrassment to a person, organization, or agency of the United States government; (iii) restrain competition; or (iv) prevent or delay the release of information the release of *which would not reasonably be expected to cause significant harm to national security*." State Secrets Policy at 2. The Attorney General also established detailed procedures — followed in this case — for review of a proposed assertion of the state secrets privilege in a particular case. Those procedures require submissions by the relevant Government departments or agencies specifying "(i) the nature of the information that must be protected from unauthorized disclosure; (ii) the significant harm to national security that disclosure can reasonably be expected to cause; (iii) the reason why unauthorized disclosure is reasonably likely to cause such harm; and (iv) any other information relevant to the decision whether the privilege should be invoked in litigation." *Id*. In addition, the Department will only defend an assertion of the privilege in court with the personal approval of the Attorney General following review and recommendations from senior Department officials. *Id*. at 3.

**B. The Attorney General Has Properly Asserted the State Secrets Privilege.**

The state secrets privilege has been properly asserted in this case. The Attorney General has formally asserted the privilege after personal consideration of the matter. *See* Declaration of Eric Holder, Attorney General ("Holder Decl."), Attached as Exhibit 1. Moreover, Joshua Skule,

Acting Assistant Director of the Counterterrorism Division of the FBI, has submitted an *in camera, ex parte* classified declaration, which attests that the disclosure of the information over which the Government asserts the privilege could reasonably be expected to cause significant harm to the national security of the United States. *See In Camera, Ex parte* Declaration of Joshua Skule ("Skule Decl."). The Government's claim of privilege is thus properly raised.

**C. Disclosure of the State Secrets Implicated by Plaintiff's Motion to Compel and over Which the Government Asserts Privilege Reasonably Could Be Expected to Cause Significant Harm to National Security.**

The United States has demonstrated in the accompanying declarations that disclosure of the information over which the Attorney General has asserted privilege reasonably could be expected to cause significant harm to national security. While "the Government need not demonstrate that injury to the national interest will inevitably result from disclosure," *Ellsberg*, 709 F.2d at 58, the showing it has made here is more than sufficient to demonstrate that the information at issue should be protected from disclosure. The Government's descriptions of the information at issue and the harms to national security at stake are fully set forth in the Skule Declaration and are also explained in the unclassified, public Declaration of Attorney General Eric H. Holder, Jr.

The Attorney General has asserted the state secrets privilege over the following categories of information, as described in unclassified terms:

- *Subject Identification*: Information that could tend to confirm or deny whether a particular individual was or was not the subject of an FBI investigation or intelligence operation. This includes the existence of any records about Plaintiff contained in the Terrorist Identities Datamart Environment ("TIDE"), which is classified in its entirety, as well as the contents of any TIDE records that might exist about Plaintiff, whether presently contained in the TIDE database or contained in any FBI counterterrorism investigative files about Plaintiff, should such exist. This also includes the contents of any FBI counterterrorism investigative or operational files about Plaintiff, should they exist.

- *Reasons for Investigation and Results*: Information that could tend to reveal the predicate for an FBI counterterrorism investigation or intelligence activity of a particular person, any information obtained during the course of such an investigation or intelligence operation, and the status and results of the investigation or operation. This includes information (if any) obtained by the FBI from the U.S. Intelligence Community related to the reasons for any investigation or operation and information regarding Plaintiff or any of his associates that could tend to reveal the predicate for, information obtained in, or results of a counterterrorism investigation or operation.

- *Sources and Methods*: Information that could tend to reveal whether particular sources and methods, such as classified policies and procedures, were used by the FBI in any counterterrorism investigation or intelligence activity (if any) of Plaintiff or his associates. This includes information related to whether court-ordered searches or surveillance, confidential human sources, and other investigative or operational sources and methods were used by the FBI in a counterterrorism investigation of or intelligence activity regarding a particular person, the reasons such methods were used, the status of the use of such sources and methods, and any results derived from such methods. In addition, this category includes the Government's Watchlisting Guidance, which sets forth the full details of how and why the Government selects individuals for watchlisting.

The Attorney General has explained in unclassified terms on the public record why the disclosure of the above information reasonably could be expected to cause significant harm to national security. Disclosure of the identities of subjects of counterterrorism investigations or intelligence activity could alert those subjects (or their associates) to the Government's interest in them and cause them to attempt to evade detection, destroy evidence, and undertake counter-actions that could put confidential informants or federal agents at risk. Holder Decl. ¶ 8. Disclosure that an individual is not the subject of an investigation, or was formerly the subject of an investigation, also presents the same risk of significant harm to national security. *Id.* ¶ 9. Confirming that someone is the subject of an investigation, while leaving the status of others unconfirmed, would enable individuals and terrorists groups alike to manipulate the system to discover whether they or their members are subject to investigation, or motivate them to act

while they know they are not being monitored. *Id.* ¶ 9. Similarly, disclosure that an individual was formerly the subject of a counterterrorism investigation could also reasonably be expected to cause significant harm to national security interests. *Id.* ¶ 10. Such disclosures provide valuable information about the Government's intelligence or could motivate a person whose previous intentions had not been detected to act. *Id.*

For closely related reasons, disclosure of the reasons for, and substance of, a counterterrorism investigation or intelligence activity reasonably could be expected to cause significant harm to national security by revealing to subjects what the FBI or U.S. Intelligence Community knows or does not know about their plans. Holder Decl. ¶¶ 11-13. Further, disclosure of the reason for an investigation could provide insights to terrorists as to what type of information is sufficient to trigger a Government inquiry, and what sources and methods the Government employs to obtain information on a person. *Id.* Disclosure of these sources and methods would reasonably be expected to cause significant harm not only by revealing the identities of particular subjects, but also by providing adversaries with insight into the specific ways in which the Government goes about detecting and preventing terrorist attacks. *Id.* ¶¶ 10-12.

Finally, disclosure of the Watchlisting Guidance, a sensitive but unclassified compilation of policies and procedures, which is drafted by the National Security Council and approved by the National Security Council Deputies Committee, could also cause significant harm to national security. Holder Decl. ¶ 14. The Guidance is disseminated solely within the watchlisting community, and has never been publicly released. *Id.* ¶ 14. The Guidance sets forth, in detail, the Government's current, comprehensive watchlist scheme related to the identification and placement of individuals in terrorism screening watchlists. *Id.* ¶ 14. If released, it would provide

a roadmap to undermine these important efforts. Thus, disclosure of the Watchlisting Guidance reasonably could be expected to cause significant harm to national security. *Id.* ¶ 14.

Defendants have fully and sufficiently demonstrated the grounds for the state secrets privilege assertion in this case, and accordingly, the privileged information described by the Attorney General, and set forth in more detail in the supporting *ex parte, in camera* Skule Declaration, should be excluded from the case. Defendants' separately-filed memorandum in support of the motion to dismiss demonstrates that the privileged information is central to resolution of the case, and the Complaint should be dismissed as a result.

## II. Defendants' Objections and Privilege Assertions Should Be Upheld and Are Sufficiently Particularized.

Plaintiff contends in his motion to compel that Defendants' objections are insufficiently particularized. *See* Motion at 2-6. This is not the case. As reflected in their responses, Defendants identified the bases on which they were either not able to provide information or noted limitations on their ability to provide it.[7]

Plaintiff's motion ignores that almost all of Defendants' interrogatory objections and answers specify the grounds for the objection, including the unreasonably long timeframe sought in the discovery requests, the range of information sought about persons other than Plaintiff, and

[7] In his motion to compel, Plaintiff does not challenge Defendants' objections to searching for and producing draft and deliberative material. Some of Plaintiff's discovery requests on their face seek information protected from disclosure by the deliberative process privilege, which must be protected in civil discovery. *See, e.g.*, RFP No. 5 (requesting information related to the "*proposed* abandonment or diminished use of the No-Fly List as a security measure"); RFP No. 6 (requesting information related to the "*proposed* increase in the use of the No-Fly List as a security measure"); RFP No. 7 (requesting information related to "*proposed* alternatives to the use of the No-Fly List") (emphasis added to all). The deliberative process privilege protects drafts, recommendations, internal analyses, and other internal documents to protect the quality and candor of administrative decision-making. *See, e.g., Dep't of Interior v. Klamath Water Users Protective Assn.*, 532 U.S. 1, 8 (2001); *City of Va. Beach v. Dep't of Commerce*, 995 F.2d 1247, 1253 (4th Cir. 1993). Plaintiff did not address this issue in his motion to compel, and the information is properly protected from disclosure.

the fact that certain information is not ordinarily tracked in the relevant databases.[8] The only interrogatory objection that Plaintiff alleges is "boilerplate" is the objection based on privileges. Plaintiff states, however, that the alleged lack of specificity with respect to this objection (and Defendants' privilege-based objections to Plaintiff's document requests) would be remedied with a privilege log and/or other specific identification and invocation of the relevant privileges. Motion at 5. This is precisely what Defendants have provided: Defendants today have lodged (*ex parte* and *in camera*) a privilege log and declarations asserting and explaining the relevant privileges and identifying the documents and information covered by the privileges.[9] Plaintiff's argument that Defendants did not identify, with the requisite specificity, the grounds upon which they rely for their objections to the document requests is also unpersuasive. Plaintiff complains that FBI and TSC listed "identical objections to virtually all of plaintiff's document requests," including objections based on the undue burden of production and the requested documents not being reasonably calculated to lead to the discovery of admissible evidence. Motion at 3-4. Plaintiff ignores, however, the request-specific portions[10] of these TSC and FBI objections.[11]

---

[8] This is in contrast to the cases Plaintiff cites that deal with wholesale failure to specify the grounds for any objections. *See Mancia v. Mayflower Textile Servs. Co.*, 253 F.R.D. 354, 363 (D. Md. 2008) (describing defendant's objections as "boilerplate, non-particularized" where there was no effort to specify the burdens or relevance issues associated with the discovery requests).

[9] Moreover, it is not surprising that Defendants asserted a variety of privileges in response to Plaintiff's discovery requests. When, as here, a lawsuit challenges the Plaintiff's alleged placement on the No Fly List--a watchlist designation designed to protect national security--potentially responsive records may well implicate classified and law enforcement information, as well as Sensitive Security Information.

[10] *See, e.g.* Motion, Exh. B-1 at 5-38 (specific objections to the wording of each request, including, for example, objection to use of the phrase "actual and/or proposed alternatives" in RFP 7); at 4 (objecting to discovery to the extent it seeks discovery not reasonably calculated to lead to the discovery of admissible evidence because the "only claims currently before the Court relate to the process by which Plaintiff was placed on the No Fly list, and this [request] sweeps beyond information and procedures considered with respect to his alleged placement, if any, on the No Fly list"); at 27 (objecting to RFP 9 as overly broad and unduly burdensome because it

Similarly unpersuasive is Plaintiff's argument that Defendants' purported failure to specify when or how they will make documents available constitutes a waiver of objections. *See* Motion at 14. At most, the cases he cites suggest that promising to produce documents at an unspecified time could be grounds for filing a motion to compel. *See Jayne H. Lee, Inc. v. Flagstaff Inds. Corp.*, 173 F.R.D. 651, 656 (D. Md. 1997); *Mezu v. Morgan State Univ.*, 269 F.R.D. 565, 574 (D. Md. 2010). They do not say anything about waiving objections, and in any event, Defendants have in fact since produced documents to Plaintiff.

## III. Information and Documents Sought by Plaintiff Have Been Properly Withheld as Irrelevant under Rule 26(b)(1) or Because Searches for the Information Requested Would Be Unduly Burdensome.

### A. Information and Documents Sought by Plaintiff Have Been Properly Withheld as Irrelevant under Rule 26(b)(1).

In his discovery requests, Plaintiff seeks a wide array of information irrelevant to his claims in both substance and time. Rule 26(b)(1) limits the scope of discovery to "nonprivileged matter that is relevant to any party's claim or defense." *Cappetta v. GC Servs. Ltd.*, No. 08-288, 2008 WL 5377934, at *2 (E.D. Va. Dec. 24, 2008); Fed. R. Civ. P. 26(b)(1). Limiting discovery to information relevant to a party's claim or defense permits the court to regulate sweeping or contentious discovery. *See* Fed. R. Civ. P. 26(b)(1), Advisory Comm. Commentary (2000 Amendments). The limitation also requires a showing of "good cause" to seek broader

---

seeks information about all persons in the TSDB who have ever filed DHS TRIP complaints, but Plaintiff has never filed for DHS TRIP and "accordingly, such information is neither relevant for Plaintiff's claims nor reasonably calculated to lead to the discovery of admissible evidence").

[11] Moreover, Defendants cannot waive the objection to documents not being in their possession, custody, or control, as the Federal Rules only provide for requests for discovery of documents that are in the opposing party's "possession, custody or control." Fed. R. Civ. P. 34(a). Similarly, Plaintiff's objection to TSC/FBI's use of "to the extent that" in its discovery responses, Motion at 3, is unavailing. Plaintiff cites no authority in support of this argument.

discovery, which must also be limited to the information that is relevant to the subject matter of the action. *Id*. Plaintiff's motion seeks numerous categories of information that are irrelevant to any party's claim or defense. The motion should be denied with respect to these requests.

**1. Information and Documents that Pre-Date Plaintiff's Alleged Inclusion on the No-Fly List**

First, although Plaintiff's claims relate to his alleged placement on the No Fly List, which he alleges to have occurred sometime after March 1, 2009, he seeks information and documents from *six years* prior to that date. *See* Interrogatories 3-16, 18 (seeking information from 2003 through the present); RFP 1-13 (seeking documents from 2003 through the present). Plaintiff offers no reason sufficient to justify such an expansive timeframe. *See Vanguard Military Equip. Corp. v. David B. Finestone Co.*, 6 F. Supp. 2d 488, 495 (E.D. Va. 1997) (interrogatory appropriately tailored to the time frame in which the fraudulent conduct was alleged to have occurred); *Melton v. Simmons*, No. 1:08-458-3, 2009 WL 454619, at *2 (W.D.N.C. Feb. 23, 2009) (denying motion to compel documents related to prior periods of confinement, not related to plaintiff's claim about current confinement).

Plaintiff's three attempts to justify the request for pre-2009 information are unpersuasive. First, although Plaintiff alleges that he was placed on the No-Fly List sometime after he left the United States (by plane) in March 2009, "in fact plaintiff only assumes he was placed on that List at that time, but he could have been placed on it years earlier." Motion at 6. Unfounded speculation cannot justify compelling an opposing party to respond to otherwise irrelevant discovery requests. *See Greenbelt Ventures, LLC v. Wash. Metro. Area Transit Auth.*, 481 F. App'x 833, 837 n.1 (4th Cir. 2012) (*per curiam*) (although plaintiff speculated that the object of the discovery it seeks must exist, plaintiff provided no colorable basis for this conclusion, and as

a result, the district court properly denied plaintiff's discovery request as nothing but a "fishing expedition.").

Next, Plaintiff argues that the 2003-2009 documents are relevant because "whatever investigatory steps defendants took" leading up to their alleged inclusion of him on the No Fly List "must have been effected before March 2009," and the "criteria and processes utilized to formulate who should be on the List . . . have changed over time, depending upon a host of factors, including political pressure." Motion at 6. Notably, though, with regard to Plaintiff's discovery requests about the criteria for inclusion on the No Fly List, Defendants responded that they would search for potentially responsive policies or procedures that were *in effect* on (*i.e.*, may pre-date) March 1, 2009, the time after which Plaintiff alleges he was placed on the No Fly List. *See* RFP 1 and 8; *see also* RFP 10 (same, for redress policies and procedures). Defendants' response thus includes any documents which are even arguably relevant to Plaintiff's alleged placement. Additionally, with regard to the request for all documents regarding Plaintiff, RFP 11, Defendants erroneously noted a temporal objection to this request. Therefore, there is no dispute on this basis because Defendants have agreed to search for pre-March 1, 2009 documents in limited instances (inclusion or redress policies related to the No Fly List; documents about Plaintiff) where they may lead to relevant information.

Finally, Plaintiff claims that the Court should compel production of pre-2009 documents and information because these would shed light on "two of the three factors in a procedural due process analysis," including the risk of erroneous deprivation through the procedures used, the probable value of additional safeguards, and the burdens of additional safeguards. Motion at 7. Plaintiff, however, fails to explain how pre-2009 documents regarding prior processes and procedures for administering the No Fly List would provide information relevant to his due

process claim. As explained above, because the only relevant procedures are those that were in place when Plaintiff was allegedly placed on the No-Fly List, whether or not pre-2009 documents would shed light on statistics correlated to a *prior version* of No Fly List procedures is ultimately immaterial to Plaintiff's claims. Plaintiff brings claims on behalf of himself, and only himself, and the Complaint contains no factual allegations related to any pre-2009 events. Discovery going back for the past eleven years is not reasonably related to the claims he asserts. For these reasons, the motion to compel production of pre-March 1, 2009 documents (save for the four exceptions already agreed to by Defendants, RFPs 1, 8, 10, 11) should therefore be denied.

**2. Discovery Requests Related to Individuals Other than Plaintiff**

Plaintiff has not brought a class action suit. Nor has he pled a claim that implicates the religion, nationality, or experiences of any individual. The discovery requests targeted at individuals other than Plaintiff (Interrogatories 7, 8, 9, 10.; RFP 8,10, 12, 18), therefore, are not sufficiently related to the operative claims and defenses in this action so as to warrant production of the requested information. *See Webb v. Green Tree Servicing LLC*, Civ. No. 11-2105, 2012 WL 3139551, at *3 (D. Md. July 27, 2012) (denying motion to compel because the requested information about tenants other than plaintiff would not yield relevant information).[12]

[12] For example, with respect to requests related to DHS TRIP, because Defendants have explained that DHS TRIP provides constitutionally adequate process, Defendants have agreed to search for and produce policies and procedures related to redress as well as final reports of any audits, investigations, or assessments about DHS TRIP. Plaintiff nonetheless seeks to compel production of all documents related to every DHS TRIP complaint related to the TSDB ever forwarded to TSC, a hugely overbroad discovery request implicating highly sensitive classified, law enforcement, and Privacy Act-protected information about other individuals not even tangentially related to the events of the Fourth Amended Complaint or any processes allegedly applied to Plaintiff. Plaintiff himself did not apply for redress through DHS TRIP, and Defendants' reasonable search is likely to find any documents even arguably relevant to Plaintiff's claims.

Plaintiff's primary argument to justify the relevance of these requests is that they are relevant to his substantive due process claim. *See* Motion at 16 ("Plaintiff believes defendants have a policy and practice of placing citizens on the No Fly List while abroad in order to coerce them into acting as informants once home. . . . Because defendants use the No Fly List in this coercive manner – to try to create this kind of leverage rather than to advance flight security – the No Fly List is plainly not narrowly tailored to advance a compelling governmental interest."). Plaintiff fails to establish that the requested information and documents about individuals other than Plaintiff are relevant to any operative claim or defense. Notably, in the substantive due process count of the Fourth Amended Complaint, Plaintiff says nothing about this alleged coercive use of the No Fly List, *see* Fourth Am. Compl. ¶¶ 58, 62, and this allegedly improper "use" therefore cannot serve as a basis for arguing that the requested information would be relevant to his claim. Moreover, to the extent Plaintiff attempts to rely on the part of the substantive due process claim alleging that he was denied a constitutional right of return in January 2011, the Court has already dismissed this claim. Mem. Op. at 27; *see also Adair v. EQT Prod. Co.*, 294 F.R.D. 1, at *6 (W.D. Va. 2013) (sustaining relevance objection to producing category of documents where plaintiffs' counsel conceded that category was relevant only insofar as a constitutional claim remained before the Court in a case, and court had already dismissed the claim seeking a declaratory judgment that a statute was unconstitutional). As a result, Defendants' relevance objections should limit any discovery in this case.

**B. Searching for the Requested Material Would Be Unduly Burdensome.**

The Court should also deny several aspects of the Motion because Plaintiff seeks to compel searches and production that would be unduly burdensome.[13] This Circuit has held that, "[e]ven assuming that this information is relevant (in the broadest sense), the simple fact that requested information is discoverable . . . does not mean that discovery must be had." *Nicholas v. Wyndham Int'l Inc.*, 373 F.3d 537, 543 (4th Cir. 2004). Though parties must produce information necessary to establish claims, courts should not permit them "to go fishing." *Surles ex rel. Johnson v. Greyhound Lines, Inc.*, 474 F.3d 288, 305 (6th Cir. 2007) (internal citations omitted). As such, courts retain discretion to determine if a discovery request is too broad or oppressive, *id*.; *see also* Fed. R. Civ. P. 26(b), and have wide discretion in balancing the needs and rights of the parties. *Surles*, 474 F.3d at 305. Specifically, the Federal Rules of Civil Procedure instruct district courts to limit discovery where the burden or expense outweighs the likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues. *See* Fed. R. Civ. P. 26(b)(2)(C)(iii); *D.J.'s Diamond Imports, LLC v. Brown*, No. WMN-11-2027, 2013 WL 1345082, at * 2, 5 (D. Md. April 1, 2013) (denying motion to compel where the value of substantive response to the interrogatory in the context of case is outweighed by "likely burden it would place on Defendant"); *Webb v. Green Tree Servicing LLC*, Civ. No. 11-2105, 2012 WL 3139551, at * 2, 5 (D. Md. July 27, 2012)

[13] Defendants objected to discovery requests on the grounds that information and documents were not in their possession and control; Plaintiff does not appear to be moving to compel such information and documents. *See, e.g.*, Motion at 9 (appearing to limit request to documents "defendants have" and requesting that "material under defendants' control which is responsive to this question should thus be produced").

(denying motion to compel where burdensome interrogatories were not relevant to proving elements of Plaintiff's claims).

**1. TSDB-Related Information**

In several of his interrogatories, Plaintiff seeks information that is not included in the TSDB. As set forth herein, and as reflected even in Plaintiff's complaint, the TSDB was created in order to provide a mechanism for sharing identifying information about persons against whom the United States should focus screening activities. The database thus includes information relevant for screening purposes, such as name, birthdate, nationality, passport number, and country of issuance. In his discovery requests, Plaintiff asks Defendants to provide him with information about persons included in the TSDB and its subset lists -- such as their citizenship status (Interrogatories 4, 7, 8, 10), religious affiliation (Interrogatory 8), place of birth/naturalization status (Interrogatory 8, 7) and the reasons why individuals were placed on and/or removed from the watchlist (Interrogatory 6, 9, 10) -- regardless of whether the TSDB tracks this information as part of its ordinary operations. *See* Declaration of G. Clayton Grigg ("Grigg Decl."), attached as Exhibit 2 (filed *ex parte* and *in camera* in full, redacted version filed herewith) ¶ 31 (TSDB does not track individuals as U.S. citizens);[14] *id.* ¶ 30 (TSDB includes a free-form field for "place of birth," but the results of any search of this field vary depending on how the information was entered; moreover, a search of this field would not provide accurate

[14] The manner by which the TSDB records citizenship status has changed over time. From 2003 through 2008, the TSDB did not track U.S. citizenship status. Grigg Decl. ¶ 31. In 2008, the TSDB began tracking individuals as USPERs, which includes both U.S. citizens and lawful permanent resident aliens. *Id.* Beginning on May 18, 2012, the TSDB also began tracking the lawful permanent resident (LPR) status of individuals; however, it did so only for individuals newly added to the TSDB. *Id.* Thus, for individuals in the TSDB prior to May 18, 2012, the TSDB did not track them by LPR status, but only by USPER/non-USPER status. *Id.* Moreover, this information is not always reliable because in some cases it is presumed based on other facts, and in other places it may be fraudulent. *Id.*

information about the places of birth of USPERS on the No Fly list because, as of this month only 26% of persons in the TSDB have a populated "place of birth" field); ¶ 35 (TSC does not, in the usual course of business, track or aggregate the basis for rejection of a nomination for inclusion in the TSDB); *see also* Motion Exh. B at 17 (TSDB does not track religious affiliation). These requests are both burdensome and unlikely to yield probative information.

First, the requests are burdensome. To obtain the information about TSDB-listed individuals that the TSDB does not track in its normal course, Defendants would need to review all of the information available as part of the individual's TSDB record, and all documentation underlying each individual's TSDB entry, including documents housed in different locations. *See* Grigg Decl. ¶ 16. While the precise number of TSDB records is sensitive, privileged information, it can be said that the number is quite large. TSC provided an artificial baseline estimate that a comprehensive review of an individual's TSDB record and the underlying information could take one hour, depending on the size and complexity of the record and other limitations.[15] *Id.* ¶ 24. For reviews of rejected nominations, using a theoretical baseline of fifteen minutes to review a record,[16] the task would require over 3,500 hours of employee time, nearly six months for four senior TSC analysts. *Id.* ¶ 36.

Second, even if such searches were not unduly burdensome, they would not be likely to yield probative information. As explained above, Plaintiff has not brought a class action suit or

[15] As noted in the Grigg Declaration, this estimate is theoretical because no review of this type has ever been attempted. Grigg Decl. ¶ 24. While uncomplicated records with minimal information, few versions, and easily accessibly underlying information could be reviewed in much less time, other record reviews can take several hours or days, depending on complexity, impediments, limitations, and other factors or circumstances. *Id.* Moreover, there is a distinct possibility that, even after exhausting all review resources, an analyst might not find responsive information at all. *Id.*

[16] This is a conservative baseline considering all the factors involved in a record review. It assumes that TSC would only review its internal records and not seek any underlying source documents. Grigg Decl. ¶ 36.

pled a claim that implicates the religion, nationality, or experiences of any individual, meaning that the discovery requests targeted at individuals other than Plaintiff (Interrogatories 7, 8, 10; RFP 8, 10, 12, 18), are not related to the operative claims and defenses in this action. Further, Defendants do not know if the information sought by Plaintiff is even included in the documents underlying a TSDB entry. For example, because the TSDB does not track a person's religion (Interrogatory 8), there is no way to identify the religion of a person on the No Fly List by looking at the TSDB entry for that person. *See* Motion, Exh. B at 17. There is also no way to know, without looking, whether that person's religion is reflected in the underlying records. *Id.* Even where religion could be guessed or surmised from the underlying records, the accuracy of any such information cannot be guaranteed. *Id.* As a result, even if Defendants could perform this search, the results would not be probative of the claims or defenses at issue in this case. The issue of burden aside, while Plaintiff suggests that the Court require a statistical sampling, Motion at 11 n.7, there is no way to know whether that sampling would ever be representative or informative.

Ultimately, what Plaintiff wants is for Defendants to create a database they do not have, and for the TSDB to track information it does not track. Plaintiff's demand that Defendants create new records in discovery is unreasonable on its face,[17] because a party responding to a Rule 34 document request cannot be compelled to prepare or create new documents. *See*

[17] It is also unreasonable to demand that Defendants produce data that is inherently unreliable. For example, Defendants should not be required to produce information derived from a field in the TSDB that is not mandatory because any conclusions drawn from the number of individuals who have information in that voluntarily completed field will be inaccurate, and therefore unlikely to provide much benefit to Plaintiff. *See* Fed. R. Civ. P. 26(b)(2)(C) (Court must limit extent of discovery where it determines that the burden or expense of the proposed discovery outweighs its likely benefit); *Brady v. Conseco, Inc.*, No. 08-05746, 2009 WL 5218046, at *2 (N.D. Cal. Dec. 29, 2009) (denying motion to compel related to interrogatories that the court found to be of marginal relevance, especially given the speculative nature of the argument defendant intended to make based on the requested information).

*Paramount Pictures Corp. v. Replay TV*, No. 01–9358, 2002 WL 32151632, at *2 (C.D. Cal. 2002). The same is true for information requested in an interrogatory response when such information is not readily accessible, such as U.S. citizenship status or the basis for removing an individual from the No Fly List. *See* Interrogatories 4, 6-10, 18. *See, e.g.*, *Kolon Indus. Inc. v. E.I. Dupont de Nemours & Co*., No. 12-1587, 2014 WL 1317695, *9-10 (4th Cir. Apr. 3, 2014) (upholding district court order finding that compilation of data from multiple sources was unduly burdensome, even if relevant). Plaintiff's belief that this information must be more readily accessible provides no basis for this Court to order production. *Susko v. City of Weirton*, No. 5:09–1, 2011 WL 98557, at *4 (N.D. W.Va. Jan. 12, 2011) (noting that "mere speculation that documents exist is not a sound basis" for permitting discovery).[18]

## IV. The Law Enforcement Privilege

Plaintiff moves to compel the production of several kinds of documents, and also to compel answers to a number of interrogatories, that Defendants are not required to provide because the requested information is protected by the law enforcement privilege.[19] The types of information sought by Plaintiff that are subject to the law enforcement privilege include (1)

[18] Plaintiff's motion does not expressly address a number of Defendants' objections and their corresponding proposals for limiting overly broad requests. Read liberally, requests for "all documents regarding assessments of the No Fly List's utility as a security measure" (RFP 4) and "all documents concerning TSC's processing of Traveler Redress Inquiry Program (TRIP) complaints" (RFP 9) encompass a huge swath of information and sweep well beyond information reasonably related to Plaintiff's alleged placement on the No Fly List. Defendants' proposed limitations include the narrowing of several document requests to "policies and procedures" (RFP 8 and 9), and the proposed exclusion of deliberative materials (RFP 2-7, 9, 12-13). Plaintiff does not challenge these reasonable limitations, by which Defendants nonetheless agreed to conduct reasonable searches for relevant policies and procedures and relevant final reports and assessments of the efficacy of the watchlisting program. Similarly, Plaintiff does not move to compel Defendants to produce documents not within their possession or control.

[19] To the extent that information is protected by overlapping privileges (such as the law enforcement privilege, or Sensitive Security Information, for example), the privileges apply independently of one another. A ruling that the one privilege is inapplicable does not foreclose the availability and protection of other privileges.

Plaintiff's status on the No Fly List (RFP 11; Interrogatory 1); (2) information about Plaintiff, if any, contained in FBI and TSC files (RFP 11; Interrogatories 1, 17); (3) the identities of FBI agents and TSC personnel (Interrogatories 1-2); (4) information about the specific criteria for inclusion in the TSDB or on the No Fly and Selectee Lists (RFP 1-10, 12-13); and (5) policies and procedures about TSC's implementation and maintenance of, as well as redress related to, the TSDB, Selectee List, and No Fly List (RFP 1-10, 12-13; Interrogatories 5, 8, 11-12). This information is properly withheld pursuant to the law enforcement privilege.[20] In support of this privilege, Defendants have submitted the *ex parte*, *in camera* declaration of John Giacalone, Assistant Director of the FBI's Counterterrorism Division.

"[L]aw enforcement agencies must be able to investigate crime without the details of the investigation being released to the public in a manner that compromises the investigation." *Va. Dep't of State Police v. Wash. Post*, 386 F.3d 567, 574 (4th Cir. 2004). "The purpose of th[e] [law enforcement] privilege is to prevent disclosure of law enforcement techniques and procedures, to preserve the confidentiality of sources, to protect witness and law enforcement personnel, to safeguard the privacy of individuals involved in an investigation, and otherwise to prevent interference with an investigation." *In re Dep't of Investigation of the City of N.Y.*, 856 F.2d 481, 484 (2d Cir. 1988). The privilege "may [also] be asserted to protect … disclosure of the contents of law enforcement investigatory files." *In re Sealed Case*, 856 F.2d 268, 271 (D.C.

[20] If the case were to go forward notwithstanding the Defendants' arguments for dismissal, as noted in Defendants' responses, there are limited, discrete pieces of unclassified information that Defendants may be willing to consider providing to Plaintiff's counsel pursuant to an appropriate protective order. *But see In Re the City of New York*, 607 F.3d 923, 936-37 (2d Cir. 2010) (describing protective orders associated with law enforcement sensitive information as "deeply flawed procedure that cannot fully protect the secrecy of information in this case; it merely mitigates—to some degree—the possibility of unauthorized disclosure."). As explained in Defendants' Motion to Dismiss, Defendants maintain that this matter cannot be properly litigated on the current record, even with the inclusion of those discrete pieces of unclassified information.

Cir. 1988). "[T]he reasons for recognizing the law enforcement privilege are even more compelling" when "the compelled production of government documents could impact highly sensitive matters relating to national security." *In re U.S. Dep't of Homeland Sec.*, 459 F.3d 565, 569 (5th Cir. 2006).

A proper review of an assertion of the law enforcement privilege involves two steps. "First, the party asserting the law enforcement privilege bears the burden of showing that the privilege indeed applies to the documents at issue" by showing that the documents contain information pertaining to law enforcement techniques and procedures, information that would undermine the confidentiality of sources, information that would endanger witness and law enforcement personnel, information that would undermine the privacy of individuals involved in the investigation, or information that would seriously impair the ability of a law enforcement agency to conduct future investigations. *In re New York City*, 607 F.3d 923, 948 (2d Cir. 2010).[21] Second, once the privilege is determined to apply, "the district court must balance the public interest in nondisclosure against 'the need of a particular litigant for access to the

[21] Plaintiff, like Defendants, cites *In re City of New York* when discussing the law enforcement privilege. *See* Motion at 5. The Fourth Circuit has not directly addressed the standard that a district court should apply to evaluate the Government's assertion of the law enforcement privilege. In the other contexts, district courts in the Fourth Circuit have looked to district court decisions in sister circuits, including the Second Circuit, for guidance. *See Martin v. Cooper*, 287 F.R.D. 348, 350-51 (D. Md. 2012) (citing, in a 42 U.S.C. § 1983 lawsuit, *King v. Conde*, 121 F.R.D. 180, 198 (E.D.N.Y. 1988)); *Wolfe v. Green*, 257 F.R.D. 109, 112 (S.D.W. Va. 2009) (same); *Bellamy-Bey v. Baltimore Police Dep't*, 237 F.R.D. 391, 393 (D. Md. 2006) (same); *Johnson v. Rankin*, Case No. 2:11-cv-0415, 2011 WL 5358056, at *1 (E.D. Va. Nov. 7, 2011) (citing, in the context of a motion to quash a subpoena duces tecum, *Frankenhauser v. Rizzo*, 59 F.R.D. 339 (E.D. Pa. 1973)); *see also Madsen v. Rogers*, Case No. 97-cv-11234, 1999 WL 651578, at *3 (E.D. Va. Jul. 20, 1999) (citing, in the context of a motion to quash a subpoena duces tecum, the law regarding the FOIA exemption for investigative information). Relative to those cases decided in other contexts, *In re City of New York* (which vacated an order compelling the production of certain sensitive law enforcement documents in a national security case) is most apposite to the issues raised in this matter. *See Martin*, 287 F.R.D. at 351 n.4 ("*In re City of New York* [is] a case involving national security [and] is distinguishable from typical § 1983 actions regarding police misconduct.").

privileged information.'" *Id.* (quoting *In re Sealed Case*, 856 F.2d at 272). There is a strong presumption against lifting the privilege that may be rebutted only by a showing that the lawsuit is non-frivolous and brought in good faith, that the information sought is not available through other discovery or from other sources, and that the party has a compelling need for the privileged information. *Id.* Third, "[i]f the presumption against disclosure is successfully rebutted [], the district court must then weigh the public interest in nondisclosure against the need of the litigant for access to the privileged information before ultimately deciding whether disclosure is required." *Id.* The information sought by Plaintiff in discovery here meets this test and is protected from disclosure by the law enforcement privilege, as set forth below and in the *ex parte, in camera* Giacalone Declaration.

First, Plaintiff requests information that would or may reveal his purported placement (and the placement of others) in the TSDB, as well as on the No Fly or Selectee Lists. *See, e.g.*, RFP 11 (all documents regarding Plaintiff); Interrogatory 1 (all persons who played any role in nominating or placing Plaintiff on the No Fly List). To the extent such information exists, its disclosure implicates information pertaining to law enforcement techniques and procedures, *see In re New York City*, 607 F.3d at 948, as well as the contents of law enforcement investigatory files, *In re Sealed Case*, 856 F.2d at 271. As set forth in the Giacalone Declaration, disclosure of watchlist status reveals sensitive law enforcement information and provides valuable information to those attempting to circumvent the law.

Second, Plaintiff seeks disclosure of all documents and information about him in the possession of the FBI and TSC. *See* RFP 11, Interrogatories 1 and 17. Yet, if such documents or information exists, they would constitute confirmation of an investigatory interest in Plaintiff, as well as demonstrate the nature and substance of any such interest, as described in the Giacalone

Declaration. *See In re Sealed Case*, 856 F.2d at 271. As a result, Plaintiff cannot show a substantial need for these records, in light of the clear law enforcement nature of such records, and the accompanying dangers from disclosure.

Third, Plaintiff requests the production of documents and information regarding the criteria for including or excluding individuals from watchlists. *See* RFP 1-10, 12-13; Interrogatory 10. As noted before, the disclosure of such criteria risks undermining the effectiveness of the watchlist. *See In re New York City*, 607 F.3d at 948. The Giacalone Declaration demonstrates that release of this information would risk circumvention of the law and cause harm to national security because disclosure of the criteria that the Government uses to nominate, add, or remove individuals from its watchlists would weaken the effectiveness of the watchlists by providing criminals and terrorists the means by which they can learn or manipulate their watchlist status.[22]

Fourth, Plaintiff requests disclosure of the policies and procedures for implementing and maintaining the watchlists, and for providing redress. *See* RFP 1-10, 12-13; Interrogatories 5, 8, 11-12. As noted before, the use of the watchlist is an effective counterterrorism tool, and disclosures about the policies and procedures for watchlisting risks undermining its effectiveness. *See In re New York City*, 607 F.3d at 948. Disclosing the policies and procedures by which the watchlists are implemented and maintained, and by which redress is provided,

[22] Moreover, Plaintiff contends he has been improperly placed on the no Fly List, but his requests seek information about the TSDB generally. This broad request for law enforcement protected information overreaches and would require Defendants to disclose sensitive information that is not implicated by Plaintiff's claims. Indeed, in an earlier decision in this case, this Court held that TSDB status (if any), standing alone, would not constitute a valid claim or provide a sufficient basis for jurisdiction. *See Mohamed v. Holder*, No. 11-50, 2011 WL 3820711, at *6 n.1, 7 (E.D. Va. Aug. 26, 2011) (concluding that a plaintiff must allege something more than mere inclusion on a watchlist to state a constitutional claim or to establish standing).

would provide a roadmap to the specific ways in which the Government identifies persons for watchlisting, as well as the ways in which that information is shared both inside and outside of the United States Government. Revealing this kind of information would weaken the Government's ability to proactively and effectively identify persons who should be watchlisted. *See generally* Giacalone Declaration. Like Plaintiff's other requests, these requests seek information far beyond Plaintiff's alleged and allegedly improper No Fly List placement and thus are not sufficiently related to his claims to justify the harms that would result from disclosure. *See supra* at III.A. [23]

**V. Sensitive Security Information**

Some of the information Plaintiff seeks in discovery also constitutes Sensitive Security Information ("SSI"), a category of information related to transportation security which is protected by statute.[24] By statute, the TSA Administrator[25] must "prescribe regulations prohibiting the disclosure of information obtained or developed in carrying out security . . . if the [Administrator] decides that disclosing the information would . . . be detrimental to the security of transportation." 49 U.S.C. § 114(r)(1)(C). Accordingly, TSA has defined SSI and set forth a

[23] Plaintiff also seeks the disclosure of the identities of law enforcement personnel involved in the allegations at issue in Complaint. The law enforcement privilege, however, protects information that would undermine the privacy of individuals involved in any law enforcement investigations, as well as information that would endanger law enforcement personnel. *See In re New York City*, 607 F.3d at 948; *see also generally* Giacalone Decl.

[24] *See* Pub. L. No. 93-366, §§ 202, 316, 88 Stat. 409, 415-17 (1974); Pub. L. No. 107-71, §101, 115 Stat. 597, 597-604 (2001) (transferring this authority from the Federal Aviation Administration to the newly created TSA).

[25] The TSA Administrator was formerly known as the Under Secretary of Transportation for Security because TSA was originally a part of the Department of Transportation. TSA's functions, as well as the Under Secretary's, were transferred to the Department of Homeland Security pursuant to section 403(2) of the Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (codified at 6 U.S.C. § 203(2)). The Under Secretary is now known as the Administrator of TSA. *See* 49 C.F.R. § 1500.3.

list of certain categories of information that are SSI. *See generally* 49 C.F.R. § 1520.5 (defining SSI and providing a list of particular categories of SSI). Plaintiff's discovery requests seek information about the No Fly and Selectee Lists and related security measures.[26] 49 C.F.R. §§ 1520.5(a)(3); 1520.5(b)(8); 1520.5(b)(9)(i) and (ii), 1520.5(b)(8); and 1520.5(b)(11).

TSA regulations limit access to SSI to "covered persons" with a "need to know." *See* 49 C.F.R. §§ 1520.7 and 1520.11. Covered persons include federal employees who have a need to know SSI if access to the information is necessary for the performance of their official duties. *See* 49 C.F.R. §§ 1520.7 and 1520.11. In order for a covered person to have access to specific SSI, that covered person must have an operational need to know, for example, "when the person requires access to specific SSI to carry out. . . transportation security activities . . .." 49 C.F.R. § 1520.11(a)(1).

Non-covered persons, such as plaintiff's counsel, do not gain access to SSI simply by filing a lawsuit. *See, e.g.*, *Chowdhury v. Nw. Airlines Corp.*, 226 F.R.D. 608, 610-15 (N.D. Cal. 2004) (holding that 49 U.S.C. §114(s), now 49 U.S.C. §114(r), creates an evidentiary privilege because it directs "the TSA to withhold disclosure of information if the TSA believes that

[26] *See, e.g.*, RFP 1, 3 (policy standards, rules, and training about the decision to include persons on the No Fly List); RFP 2 (reviews and audits of the No Fly List); RFP 4, 5, 6 (assessments and reviews of the utility of No Fly List as a security measure); RFP 7 (No Fly List alternatives); Interrogatories 11, 12, 17 (safety measures associated with flights bearing persons allegedly on the No Fly List). These requests track the categories of SSI reflected in TSA's SSI regulation. *See, e.g.,* 49 C.F.R. § 1520.5(b)(9)(i), (ii) (reflecting that SSI includes "security programs and contingency plans"; "[d]etails of any security inspection or investigation of an alleged violation of aviation, maritime, or rail transportation security requirements of Federal law that could reveal a security vulnerability, including the identity of the Federal special agent or other Federal employee who conducted the inspection or audit"; "Security screening information"; "Any procedures, including selection criteria and any comments, instructions, and implementing guidance pertaining thereto, for screening of persons, accessible property, checked baggage, U.S. mail, stores, and cargo, that is conducted by the Federal government or any other authorized person.").

disclosure would be detrimental to air transportation safety," unless TSA issues regulations permitting such disclosure when it is not deemed harmful). As a general matter, SSI may not be disclosed to a non-covered person except with the express consent of the TSA Administrator or his designee. *See* 49 C.F.R. § 1520.9(a)(2). Further, TSA's designation of information as SSI is reviewable only in the United States Courts of Appeals – not in United States District Courts. 49 U.S.C. § 46110(a).[27]

In the context of civil litigation in federal district court, Congress has created a statutory mechanism that allows for the possibility that individuals, who are not otherwise covered persons with a need to know, may obtain access to certain SSI subject to specific conditions and strict controls. Section 525(d) of the DHS Appropriations Act, 2007, Pub. L. 109-295, § 525(d), 120 Stat. 1355 (Oct. 4, 2006), as reenacted, ("Section 525(d)")[28] provides that a party or party's counsel seeking access to specific SSI must demonstrate to TSA a substantial need for relevant SSI in the preparation of their case and further show that they are unable without undue hardship to obtain the substantial equivalent of the information by other means. In addition, such individuals must successfully undergo a criminal history check and terrorist threat assessment like that performed for aviation workers, and the district court must enter a protective order that protects the SSI from unauthorized or unnecessary disclosure.[29] Section 525(d) further provides

---

[27] *See, e.g., Lacson v. U.S. Dep't of Homeland Sec.*, 726 F.3d 170, 172 (D.C. Cir. 2013); *Robinson v. Napolitano*, 689 F.3d 888 (8th Cir. 2012); *MacLean v. Dep't of Homeland Sec.*, 543 F.3d 1145, 1149 (9th Cir. 2008).

[28] Section 525 has never been codified, but Section 525(d) has been reenacted in each subsequent act of Congress providing appropriations to the Department of Homeland Security. *See, e.g.*, Consolidated Appropriations Act, 2008, Pub. L. No. 110-161, Div. E, § 522, 121 Stat. 1844, 2073-74 (Dec. 26, 2007); Consolidated Appropriations Act of 2014, Pub. L. No. 113-76, Div. F, § 510 (Jan. 17, 2014).

[29] In addition, the Secretary of DHS may assess a civil penalty of up to $50,000 for each violation of 49 C.F.R. Part 1520 by persons provided access to SSI under Section 525(d). See § 525(d), 120 Stat. at 1382.

that any order granting access to SSI is immediately appealable to the United States Courts of Appeal.

Although two of Plaintiff's current counsel have passed background checks in connection with proceedings in the Court of Appeals, pursuant to 49 C.F.R. § 1520.15(e), such checks alone are insufficient to permit disclosure of SSI to them. Section 525(d) requires that the Court must first enter a protective order that protects SSI from "unauthorized or unnecessary disclosure and specifies the terms and conditions of access." To date, no such protective order has been entered by the Court and, as a result, Defendants are prohibited by law from disclosing SSI to Plaintiff's counsel. Moreover, given the Government's motion to dismiss this case in light of the scope of the state secrets privilege, there is no reason for the Court to enter such an order at this time. In the event that this Court determines that the case can proceed, in spite of the Government's arguments about the scope of the state secrets privilege, Defendants are prepared to propose a protective order that protects SSI and specifies the terms and conditions of access. If such a protective order is entered, Plaintiff's counsel would be required to satisfy the other requirements of Section 525(d). In the meantime, Defendants have attempted to identify (among other privileges) materials containing SSI on their privilege log but are prohibited from producing them. 49 C.F.R. § 1520.(9)(a)(2). In the event that this case proceeds, and such materials are required to be produced, they must be referred to TSA for review as required by regulation. 49 C.F.R. § 1520.5(a)(9)(3). In the event discovery does proceed, and the requirements of Section 525(d) are met, TSA security experts will conduct a line-by-line review of any such documents to identify with specificity the SSI contained therein.

**CONCLUSION**

For the foregoing reasons, the Court should deny the motion to compel.

Dated: May 28, 2014

Respectfully submitted,

STUART F. DELERY
ASSISTANT ATTORNEY GENERAL
CIVIL DIVISION

DANA J. BOENTE
UNITED STATES ATTORNEY

DIANE KELLEHER
ASSISTANT BRANCH DIRECTOR
FEDERAL PROGRAMS BRANCH

AMY E. POWELL
JOSEPH C. FOLIO, III
ATTORNEYS
U.S. DEPARTMENT OF JUSTICE
CIVIL DIVISION, FEDERAL PROGRAMS BRANCH
20 MASSACHUSETTS AVENUE, N.W.
WASHINGTON, D.C. 20001
TELEPHONE: (202) 514-9836
FAX: (202) 616-8460
E-MAIL: amy.powell@usdoj.gov

/S/
R. JOSEPH SHER
ASSISTANT UNITED STATES ATTORNEY
OFFICE OF THE UNITED STATES ATTORNEY
JUSTIN W. WILLIAMS UNITED STATES ATTORNEYS BUILDING
2100 JAMIESON AVE.,
ALEXANDRIA, VA. 22314
TELEPHONE: (703) 299-3747
FAX: (703) 299-3983
E-MAIL JOE.SHER@USDOJ.GOV

ATTORNEYS FOR THE DEFENDANTS

CERTIFICATE OF SERVICE

I certify that I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of such filing (NEF) to the following counsel of record:

Gadeir Abbas
Nina Kraut
THE COUNCIL ON AMERICAN- ISLAMIC RELATIONS
453 New Jersey Avenue, SE
Washington, D.C. 20003
Telephone: (202) 742-6410
Fax: (202) 488-0833
Email: gabbas@cair.com
Email: nkraut@cair.com

DATED: MAY 28, 2014

/S/
R. JOSEPH SHER
ASSISTANT UNITED STATES ATTORNEY
OFFICE OF THE UNITED STATES ATTORNEY
JUSTIN W. WILLIAMS UNITED STATES ATTORNEYS' BUILDING
2100 JAMIESON AVE.,
ALEXANDRIA, VA. 22314
TELEPHONE: (703) 299-3747
FAX: (703) 299-3983
E-MAIL JOE.SHER@USDOJ.GO

**UNITED STATES DISTRICT COURT**
**EASTERN DISTRICT OF VIRGINIA**
**ALEXANDRIA DIVISION**

| | | |
|---|---|---|
| GULET MOHAMED, | ) | |
| Plaintiff, | ) | |
| v. | ) | Case No. 1:11-CV-0050 |
| ERIC H. HOLDER, JR., in his official capacity as Attorney General of the United States, *et al*., | ) | |
| Defendants. | ) | |

**DEFENDANTS' MEMORANDUM OF LAW**
**IN OPPOSITION TO PLAINTIFF'S MOTION TO COMPEL**

**EXHIBIT 1 – DECLARATION OF ERIC H. HOLDER, JR.**

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

GULET MOHAMED,

PLAINTIFF,

v.

ERIC H. HOLDER, JR., IN HIS OFFICIAL CAPACITY AS ATTORNEY GENERAL OF THE UNITED STATES, *ET AL.*,

DEFENDANTS.

Case No. 1:11-CV-00050

**DECLARATION OF ERIC H. HOLDER, JR., ATTORNEY GENERAL OF THE UNITED STATES**

I, ERIC H. HOLDER, JR., hereby state and declare as follows:

1. I am the Attorney General of the United States and head of the United States Department of Justice ("DOJ"), an Executive Department of the United States. *See* 28 U.S.C §§ 501, 503, 509. The purpose of this declaration is to assert, at the request of the Federal Bureau of Investigation ("FBI"), and in my capacity as Attorney General and head of DOJ, a formal claim of the state secrets privilege in order to protect the national security interests of the United States. The statements made herein are based on my personal knowledge, on information provided to me in my official capacity, and on my evaluation of that information.

2. In the course of my official duties, I have been informed that Plaintiff Gulet Mohamed, 21 years old, is a naturalized U.S. citizen. He left the United States in 2009 and traveled in Yemen, Somalia, and Kuwait. I understand that Plaintiff claims that he was interrogated and tortured, allegedly with the complicity of unknown U.S. officials. I further understand that in

January 2011, he was denied boarding on a flight returning to the United States, but that shortly after, he did return to the United States., and he has been here since that time.

3. I understand that Plaintiff asserts that his name is currently on the No Fly List, and he seeks declaratory relief finding that the placement of his name on the list violates his Fifth and Fourteenth Amendment rights under the United States Constitution and the Administrative Procedures Act, and injunctive relief ordering, among other things, Defendants to give him notice of his inclusion on any Government watchlist, an opportunity to rebut evidence underlying that inclusion, removal from any watchlist that affected his ability to return to United States, as well as compensatory and punitive damages.

4. I am advised that the Plaintiff seeks through discovery the production of classified and otherwise privileged information and has also filed a motion to compel this information in discovery. Defendants are opposing that motion and asserting applicable privileges. As described below, the disclosure of the information sought by Plaintiff through his discovery could reasonably be expected to cause significant harm to the national security.

5. I have read and carefully considered the classified declaration of Joshua Skule, Acting Assistant Director, Counterterrorism Division of the FBI. After careful and personal consideration of the matter, I have concluded that disclosure of the three categories of information described below, and in more detail in the classified FBI declaration, could reasonably be expected to cause significant harm to the national security, and I therefore formally assert the state secrets privilege over this information. The classified FBI declaration, which is available for the Court's *ex parte, in camera* review, describes in classified detail the information over which I am asserting the state secrets privilege. As Attorney General, I possess

original classification authority under Section 1.3 of Executive Order (E.O. 13526) dated December 29, 2009. *See* 75 Fed. Reg. 707. I have determined that the classified FBI declaration is properly classified under Section 1.2 of E.O. 13526 because public disclosure of the information contained in that declaration also could reasonably be expected to cause significant harm to national security.

6. In unclassified terms, my privilege assertion encompasses information in the following categories:

- *Subject Identification*: Information that could tend to confirm or deny whether a particular individual was or was not the subject of an FBI investigation or intelligence operation. This includes the existence of any records about Plaintiff contained in the Terrorist Identities Datamart Environment ("TIDE"), which is classified in its entirety, as well as the contents of any TIDE records that might exist about Plaintiff, whether presently contained in the TIDE database or contained in any FBI counterterrorism investigative files about Plaintiff, should such exist. This also includes the contents of any FBI counterterrorism investigative or operational files about Plaintiff, should they exist.

- *Reasons for Investigation and Results*: Information that could tend to reveal the predicate for an FBI counterterrorism investigation or intelligence activity of a particular person, any information obtained during the course of such an investigation or intelligence operation, and the status and results of the investigation or operation. This includes information (if any) obtained by the FBI from the U.S. Intelligence Community related to the reasons for any investigation or operation and information regarding Plaintiff or any of his associates that could tend to reveal the predicate for, information obtained in, or results of a counterterrorism investigation or operation.

- *Sources and Methods*: Information that could tend to reveal whether particular sources and methods, such as classified policies and procedures, were used by the FBI in any counterterrorism investigation or intelligence activity (if any) of Plaintiff or his associates. This includes information related to whether court-ordered searches or surveillance, confidential human sources, and other investigative or operational sources and methods were used by the FBI in a counterterrorism investigation of or intelligence activity regarding a particular person, the reasons such methods were used, the status

of the use of such sources and methods, and any results derived from such methods. In addition, this category includes the Government's Watchlisting Guidance, which sets forth the full details of how and why the Government selects individuals for watchlisting.

7. As indicated above and explained further below, I have determined that disclosure of information falling into the foregoing categories could reasonably be expected to cause significant harm to national security.

8. First, I concur with the determination of the FBI that the disclosure of the identities of subjects of FBI counterterrorism investigations or intelligence activity reasonably could be expected to cause significant harm to national security. As the FBI has explained, such disclosures would alert those subjects to the Government's interest in them and could cause them to attempt to flee, destroy evidence, or alter their conduct so as to avoid detection of their future activities, which would seriously impede law enforcement and intelligence officers' ability to determine their whereabouts or gain further intelligence on their activities. In addition, as the FBI has explained, knowledge that they were under investigation could enable subjects to anticipate the actions of law enforcement and intelligence officers, possibly leading to counter-surveillance that could place federal agents at higher risk, and to ascertain the identities of confidential informants or other intelligence sources, placing those sources at risk. Such knowledge could also alert associates of the subjects to the fact that the Government is likely aware of their associations with the subjects and cause them to take similar steps to avoid scrutiny.

9. Second, I agree with the FBI that disclosure that an individual is not a subject of an FBI counterterrorism investigation could likewise reasonably be expected to cause significant harm

to national security. As the declaration explains, if the fact that some persons are not subject to investigation is disclosed, while the status of others is left unconfirmed, the disclosure would reveal that the FBI has had an investigative interest as to those other particular persons. Allowing such disclosures would enable individuals and terrorist groups alike to manipulate the system to discover whether they or their members are subject to investigation. Further, individuals who desire to commit terrorist acts could be motivated to do so upon discovering that they are not being monitored.

10. In addition, I agree with the judgment of the FBI that where an investigation of a subject has been closed, disclosure that an individual was formerly the subject of an FBI counterterrorism investigation or intelligence activity could also reasonably be expected to cause significant harm to national security. Again, I agree that, to the extent that an individual had terrorist intentions that were not previously detected, the knowledge that he or she is no longer the subject of investigative or intelligence interest could embolden him or her to carry out those intentions. Moreover, as the FBI indicates, the fact that an investigation is closed does not mean that the subjects have necessarily been cleared of wrongdoing, as closed cases are often reopened based on new information. Even if the former subjects are law abiding, the disclosure that they had been investigated could still provide valuable information to terrorists and terrorist organizations about the Government's intelligence and concerns, particularly where the former subjects have associates whom the FBI may still be investigating based on suspected ties to terrorist activity. Disclosure of the FBI's interest in the closed subject could alert such associates to the interest in them and lead them to destroy evidence or alter their conduct so as to avoid detection of their future activities.

11. Third, I agree with the judgment of the FBI that disclosure of the reasons for and results from an FBI counterterrorism investigation or an intelligence activity --- whether the initial predicate for opening an investigation, information gained during the investigation, or the status or results of the investigation --- could also reasonably be expected to cause significant harm to national security. As the FBI has determined, such disclosures would reveal to subjects who are involved in or planning to undertake terrorist activities what the FBI or the intelligence community knows or does not know about their plans and the threat they pose to national security. Even if the subjects have no terrorist intentions, disclosure of the reasons they came under investigation may reveal sensitive intelligence information about them, their associates, or a particular threat that would harm other investigations. More generally, as the FBI also explains, disclosure of the reasons for an investigation could provide insights to persons intent on committing terrorist attacks as to what type of information is sufficient to trigger an inquiry by the United States Government, and what sources and methods the FBI may employ to obtain information about a person.

12. I also agree with the FBI that the disclosure of certain information that would tend to describe, reveal, confirm or deny the existence or use of FBI investigative or sources and methods, or techniques used in the counterterrorism investigations at issue in this case, could likewise be reasonably expected to cause significant harm to national security. This aspect of my privilege assertion includes information that would tend to reveal whether court-ordered searches or surveillance, confidential human sources, and other investigative sources and methods were used in a counterterrorism investigation of a particular person, the reasons for and the status of the use of such sources and methods, and any results derived from such methods. The disclosure

of such information could reveal not only the identities of particular subjects but also the steps taken by the FBI in counterterrorism matters.

13. Any effort to draw distinctions between disclosures that would and those that would not cause harm to national security interests would itself reveal sensitive FBI counterterrorism investigative or intelligence information. If the Government were to disclose that one individual is not now nor ever has been the subject of an investigation, but resist such disclosure when an individual is currently or once was the subject of a national security investigation, then the very act of resisting disclosure would itself reveal the information that the Government seeks to protect. For this reason, the information at issue --- whether someone is, is no longer, or never has been the subject of an FBI counterterrorism investigation --- must be treated uniformly. Any type of disclosure, whether affirmative or negative, would implicate the harms described above.

14. Finally, I agree with the FBI that the Watchlisting Guidance, although unclassified, contains national security information that, if disclosed, for the reasons discussed in the FBI's classified declaration, could cause significant harm to national security. The Guidance is coordinated by the National Security Council ("NSC") and approved by the Deputies Committee, which is an NSC Committee comprised of deputies to members of the President's Cabinet. The Guidance is disseminated solely within the U.S. Government watchlisting and screening communities and only to those who possess a need to know such information. The Guidance is unclassified in order to facilitate information-sharing among U.S. Government agencies involved in watchlisting and screening efforts. It has never been publicly released. The Guidance sets forth, in detail, the Government's comprehensive watchlist scheme related to the identification and placement of individuals in terrorism screening watchlists. If the Guidance

were released, it would provide a clear roadmap to undermine the Government's screening efforts, a key counterterrorism measure, and thus, its disclosure reasonably could be expected to cause significant harm to national security.

15. Any further elaboration concerning the foregoing matters on the public record would reveal information that could cause the very harms my assertion of the state secrets privilege is intended to prevent. The classified FBI declaration, submitted for *ex parte, in camera* review, provides a more detailed explanation of the information over which I am asserting the privilege and the harms to national security that would result from disclosure of that information.

16. On September 23, 2009, I announced a new Executive Branch policy governing the assertion and defense of the state secrets privilege in litigation. Under this policy, the Department of Justice will defend an assertion of the state secrets privilege in litigation, and seek dismissal of a claim on that basis, only when necessary to protect against the risk of significant harm to national security. *See* Exhibit 1 (State Secrets Policy), § 1(A). The policy provides further that an application of a privilege assertion must be narrowly tailored and that dismissal be sought pursuant to the privilege assertion only when necessary to prevent significant harm to national security. *Id.* § 1(B). Moreover, "[t]he Department will not defend an invocation of the privilege in order to: (i) conceal violations of the law, inefficiency, or administrative error; (ii) prevent embarrassment to a person, organization, or agency of the United States Government; (iii) restrain competition; or (iv) prevent or delay the release of information the release of which would not reasonably be expected to cause significant harm to national security." *Id.* § 1(C). The policy also establishes detailed procedures for review of a proposed assertion of the state secrets privilege in a particular case. *Id.* § 2. Those procedures require submissions by the

relevant Government departments or agencies specifying "(i) the nature of the information that must be protected from unauthorized disclosure; (ii) the significant harm to national security that disclosure can reasonably be expected to cause; [and] (iii) the reason why unauthorized disclosure is reasonably likely to cause such harm." *Id.* § 2(A). Based on my personal consideration of the matter, I have determined that the requirements for an assertion and defense of the state secrets privilege have been met in this case in accord with the September 2009 State Secrets Policy.

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

Executed this 27 day of May, 2014, in Washington, D.C.

ERIC H. HOLDER, JR.
ATTORNEY GENERAL OF THE UNITED STATES

# Exhibit 1

# Office of the Attorney General
## Washington, D. C. 20530

September 23, 2009

*MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES*
MEMORANDUM FOR THE HEADS OF DEPARTMENT COMPONENTS

FROM: THE ATTORNEY GENERAL

SUBJECT: Policies and Procedures Governing Invocation of the State Secrets Privilege

I am issuing today new Department of Justice policies and administrative procedures that will provide greater accountability and reliability in the invocation of the state secrets privilege in litigation. The Department is adopting these policies and procedures to strengthen public confidence that the U.S. Government will invoke the privilege in court only when genuine and significant harm to national defense or foreign relations is at stake and only to the extent necessary to safeguard those interests. The policies and procedures set forth in this Memorandum are effective as of October 1, 2009, and the Department shall apply them in all cases in which a government department or agency thereafter seeks to invoke the state secrets privilege in litigation.

**1. Standards for Determination**

**A. Legal Standard.** The Department will defend an assertion of the state secrets privilege ("privilege") in litigation when a government department or agency seeking to assert the privilege makes a sufficient showing that assertion of the privilege is necessary to protect information the unauthorized disclosure of which reasonably could be expected to cause significant harm to the national defense or foreign relations ("national security") of the United States. With respect to classified information, the Department will defend invocation of the privilege to protect information properly classified pursuant to Executive Order 12958, as amended, or any successor order, at any level of classification, so long as the unauthorized disclosure of such information reasonably could be expected to cause significant harm to the national security of the United States. With respect to information that is nonpublic but not classified, the Department will also defend invocation of the privilege so long as the disclosure of such information reasonably could be expected to cause significant harm to the national security of the United States.

**B. Narrow Tailoring.** The Department's policy is that the privilege should be invoked only to the extent necessary to protect against the risk of significant harm to national security. The Department will seek to dismiss a litigant's claim or case on the basis of the state secrets privilege only when doing so is necessary to protect against the risk of significant harm to national security.

**C. Limitations.** The Department will not defend an invocation of the privilege in order to: (i) conceal violations of the law, inefficiency, or administrative error; (ii) prevent embarrassment to a person, organization, or agency of the United States government; (iii) restrain competition; or (iv) prevent or delay the release of information the release of *which would not reasonably be expected to cause significant harm to national security.*

## 2. Initial Procedures for Invocation of the Privilege

**A. Evidentiary Support.** A government department or agency seeking invocation of the privilege in litigation must submit to the Division in the Department with responsibility for the litigation in question[1] a detailed declaration based on personal knowledge that specifies in detail: (i) the nature of the information that must be protected from unauthorized disclosure; (ii) the significant harm to national security that disclosure can reasonably be expected to cause; (iii) the reason why unauthorized disclosure is reasonably likely to cause such harm; and (iv) any other information relevant to the decision whether the privilege should be invoked in litigation.

**B. Recommendation from the Assistant Attorney General**. The Assistant Attorney General for the Division responsible for the matter shall formally recommend in writing whether or not the Department should defend the assertion of the privilege in litigation. In order to make a formal recommendation to defend the assertion of the privilege, the Assistant Attorney General must conclude, based on a personal evaluation of the evidence submitted by the department or agency seeking invocation of the privilege, that the standards set forth in Section 1(a) of this Memorandum are satisfied. The recommendation of the Assistant Attorney General shall be made in a timely manner to ensure that the State Secrets Review Committee has adequate time to give meaningful consideration to the recommendation.

## 3. State Secrets Review Committee

**A. Review Committee.** A State Secrets Review Committee consisting of senior Department of Justice officials designated by the Attorney General will evaluate the

[1] The question whether to invoke the privilege typically arises in civil litigation. Requests for invocation of the privilege in those cases shall be addressed to the Civil Division. The question whether to invoke the privilege also may arise in cases handled by the Environment and Natural Resources Division (ENRD), and requests for invocation of the privilege shall be addressed to ENRD in those instances. It is also possible that a court may require the Government to satisfy the standards for invoking the privilege in criminal proceedings. *See United States v. Araf*, 533 F.3d 72, 78-80 (2d Cir. 2008); *but see United States v. Rosen*, 557 F.3d 192, 198 (4th Cir. 2009). In such instances, requests to submit filings to satisfy that standard shall be directed to the National Security Division.

Assistant Attorney General's recommendation to determine whether invocation of the privilege in litigation is warranted.

**B. Consultation.** The Review Committee will consult as necessary and appropriate with the department or agency seeking invocation of the privilege in litigation and with the Office of the Director of National Intelligence. The Review Committee must engage in such consultation prior to making any recommendation against defending the invocation of the privilege in litigation.

**C. Recommendation by the Review Committee.** The Review Committee shall make a recommendation to the Deputy Attorney General, who shall in turn make a recommendation to the Attorney General.[2] The recommendations shall be made in a timely manner to ensure that the Attorney General has adequate time to give meaningful consideration to such recommendations.

**4. Attorney General Approval**

**A. Attorney General Approval.** The Department will not defend an assertion of the privilege in litigation without the personal approval of the Attorney General (or, in the absence or recusal of the Attorney General, the Deputy Attorney General or the Acting Attorney General).

**B. Notification to Agency or Department Head.** In the event that the Attorney General does not approve invocation of the privilege in litigation with respect to some or all of the information a requesting department or agency seeks to protect, the Department will provide prompt notice to the head of the requesting department or agency.

**C. Referral to Agency or Department Inspector General.** If the Attorney General concludes that it would be proper to defend invocation of the privilege in a case, and that invocation of the privilege would preclude adjudication of particular claims, but that the case raises credible allegations of government wrongdoing, the Department will refer those allegations to the Inspector General of the appropriate department or agency for further investigation, and will provide prompt notice of the referral to the head of the appropriate department or agency.

[2] In civil cases, the review committee's recommendation should be made through the Associate Attorney General to the Deputy Attorney General, who shall in turn make a recommendation to the Attorney General.

**5. Reporting to Congress**

The Department will provide periodic reports to appropriate oversight committees of Congress with respect to all cases in which the Department invokes the privilege on behalf of departments or agencies in litigation, explaining the basis for invoking the privilege.

**6. Classification Authority**

The department or agency with classification authority over information potentially subject to an invocation of the privilege at all times retains its classification authority under Executive Order 12958, as amended, or any successor order.

**7. No Substantive or Procedural Rights Created**

This policy statement is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

**UNITED STATES DISTRICT COURT**
**EASTERN DISTRICT OF VIRGINIA**
**ALEXANDRIA DIVISION**

| | | |
|---|---|---|
| GULET MOHAMED, | ) | |
| Plaintiff, | ) | |
| v. | ) | Case No. 1:11-CV-0050 |
| ERIC H. HOLDER, JR., in his official capacity as Attorney General of the United States, *et al*., | ) | |
| Defendants. | ) | |

**DEFENDANTS' MEMORANDUM OF LAW**
**IN OPPOSITION TO PLAINTIFF'S MOTION TO COMPEL**

**EXHIBIT 2 – DECLARATION OF G. CLAYTON GRIGG**

~~UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE~~
~~SENSITIVE SECURITY INFORMATION~~

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

GULET MOHAMED,

*Plaintiff*,

v.

ERIC H. HOLDER, JR., *et al.*,

*Defendants*.

Case No. 11-CV-00050

**DECLARATION OF G. CLAYTON GRIGG**
**SUBMITTED IN CAMERA, EX PARTE**

I, G. Clayton Grigg, hereby declare:

1. (U) I am the Deputy Director for Operations of the Terrorist Screening Center (TSC). I became Deputy Director at TSC in September 2013. I have been a Special Agent with the Federal Bureau of Investigation (FBI) since 1997 and have served in a variety of criminal investigative, counterterrorism, and senior management positions.

2. (U) This declaration is based on my personal knowledge and my review and consideration of information available to me in my official capacity, including information furnished by TSC



~~UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE~~
~~SENSITIVE SECURITY INFORMATION~~

personnel, FBI Special Agents, Federal Air Marshals, and/or other government agency employees or contract employees in the course of their official duties.

3. (U) Each paragraph in this declaration is marked with letters indicating the level of classification and restrictions on dissemination applicable to that paragraph. Paragraphs marked with a "U" are unclassified. Paragraphs marked with "LES" are considered to be Law Enforcement Sensitive. Paragraphs marked with "SSI" are considered Sensitive Security Information.

4. (U) I am aware that plaintiff has asked the Court to compel the defendants, including the TSC, to respond more fully to Plaintiff's interrogatories and to produce documents responsive to Plaintiff's requests for production. I verified the responses to the Plaintiff's First Set of Interrogatories. I make this declaration to apprise the Court of the nature and scope of information contained in the Terrorist Screening Database (TSDB), and thereby explain how unduly burdensome the search for and production of the information sought by Plaintiff would be.

## (U) OVERVIEW OF THE CONSOLIDATED U.S. TERRORIST WATCHLIST

5. (U) The TSDB is the federal government's consolidated terrorist watchlist. The TSDB contains names and other identifying information, such as name and date of birth of

individuals known or suspected to be or to have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism. The TDSB does not contain the underlying classified intelligence or other sensitive law enforcement information that is the basis for the individual's inclusion in the database.

6. (U) The TSDB was created and is maintained by TSC, a multi-agency federal government center administered by the FBI. TSC receives identity information about domestic terrorists from the FBI. Identity information about suspected international terrorists is supplied by the National Counterterrorism Center (NCTC), which serves as the central agency for gathering and analyzing intelligence obtained by the U.S. Government pertaining to international terrorism.

7. (U) Upon receipt of this identity information, TSC reviews these nominations received from the FBI and NCTC, and conducts a review of the underlying intelligence or information that demonstrates the nature of an individual's or group's association with terrorism or terrorist activities maintained by those entities to determine whether an individual meets the criteria for inclusion in the TSDB (this underlying information is known as derogatory information or "derog"). Inclusion generally requires a determination that there is reasonable suspicion to believe that the individual is known or suspected to be or have engaged in conduct

constituting, in preparation for, in aid of, or related to terrorism.[1] That determination must be made on the basis of objective factual information.

8. (U//LES) [redacted]

9. (U//LES/SSI) [redacted]

[1] (U//LES) [redacted]

[redacted]

10. (U//LES/SSI) [redacted]

11. (U//LES/SSI) [redacted]

12. (U) TSC and the nominating agencies seek to ensure the continuing accuracy of the information in the TSDB. An intelligence or law enforcement agency that nominated an

individual to the TSDB because of suspected ties to international terrorism must promptly notify the NCTC of any information that might require modification or deletion of an individual from the TSDB, and the NCTC must then transmit that information to TSC. The FBI is likewise required to promptly notify TSC if it receives information suggesting the need to modify or delete a record from the TSDB with respect to an individual suspected of links to domestic terrorism.

13. (U) In addition to these required reviews by the nominating agencies, TSC performs its own reviews of the records of individuals included in the TSDB to verify that there is adequate support for the inclusion of an individual in the database. At the outset, as previously discussed, TSC conducts a review when an individual is newly nominated for inclusion in the TSDB, which is referred to as an "ADD" nomination. The TSC may conduct additional reviews of the records of an individual included in the TSDB on other occasions. When a person in the TSDB is encountered—for example, when attempting to board a U.S.-bound flight—and the encounter yields new or previously unknown information, the TSC will conduct a review of that person's record. Similarly, if TSC is provided with new intelligence or with any changes to the biographic, biometric or derogatory information for an individual in the TSDB, TSC conducts a review of that person's records. In both instances, any

resulting modifications or changes are referred to as a "MODIFY" nomination. Separately, the TSC provides USPERS included in the TSDB with an additional layer of analysis by conducting bi-annual reviews of all USPER records. This review consists of an analytical assessment of the underlying derogatory information that supports the USPER's watchlisting status.

14. (U//LES/SSI) [redacted]

[redacted]

15. (U) The TSDB has some "free form" input fields, which means that they do not follow a specific recognized template for information such as a "(123) 456-7890" phone number standard or a "123-45-6789" standard for recording social security numbers. By the very nature of a free form input field, although TSC is able to search for information entered into such a field, the fields are not optimized for tracking of specific types of information. Free form input fields are text boxes which allow users to input unstructured text without restricting parameters other than the total number of characters. For example, in the "Place of Birth" field (which is not a required TSDB field), information entered in this field ranges from no information, to cities, to country abbreviations (e.g., New York, United States, US or USA). Additionally, in certain circumstances, there may be multiple different inputs in the field. Although an individual can have only one place of birth, many records contain multiple entries in this field, based on reporting from the underlying source documents. In cases in which an individual claims multiple identities and uses conflicting information, all identifiers, whether fraudulent or not, are included in the TSDB. Consequently, the type and form of information entered in free form fields (if anything is entered at all) can vary greatly and the accuracy and consistency of any search cannot be guaranteed. The fact of free form input fields makes searches (and therefore some interrogatory responses) more burdensome

and impractical, if not impossible. Searching for a key term would be limited by the information in the field; and only information in the field matching the search term would be recognized. Searches for interrogatory responses would be at best incomplete and full accuracy could only be achieved by manual searches of all records.

**(U) BURDEN ASSOCIATED WITH A REVIEW OF INFORMATION NOT TRACKED IN THE TSDB**

16. (U) When Plaintiff seeks information that is not tracked by, or is not available in the TSDB, any attempt by TSC to discover the information requested would require the expenditure of a substantial amount of resources. A search for information not tracked by or available in the TSDB would require a review of two separate classes of information: (a) the information available as part of an individual's TSDB record; and, (b) the "derogatory" information underlying an individual's nomination to the TSDB, which may be found in a multitude of locations. A search for the information requested by Plaintiff through each of these classes of information would involve several different layers of review. The volume and specificity of the search requested also adds to the substantial burden.

**(U) BURDEN ASSOCIATED WITH A COMPREHENSIVE REVIEW OF A TSDB RECORD**

17. (U) With regard to information available as part of an individual's TSDB record, an analyst's search for the requested information would begin with a review of all of the information in a person's TSDB record (i.e., all information included in the TSDB about a person). A typical record includes all available information (including that which is at a minimum required to conduct effective screening and any additional information provided or added thereto) entered about that person as of the date that the TSDB is reviewed. See, e.g., Exh. 2 at 7 (sample TSDB entry). In some instances, a review of the entire record may not be required because it is possible that an answer may be readily determined from a brief review of the record. In other instances, though, the requested information will not be apparent or exist at all, and so an analyst must review carefully the entirety of a person's record.

18. (U) In addition to the most current record, however, the TSDB, since 2006, also includes all prior versions of a person's record. Each time a record is edited, the TSDB saves the record as a new version. Therefore, in order to review all information about a person in the TSDB, an analyst must review not only the current version of the record for a person in the TSDB, but also all previous versions of that person's TSDB record that are available. The number of versions of a record for a person in the TSDB can vary widely, but some individuals may

have several hundred different versions. Currently, there is no way for the TSC to determine efficiently the difference between each of these versions without a version-by-version review; each version must be reviewed to determine what changes to the record occurred with that version.

19. (U) The burden of reviewing an individual's TSDB record would vary depending on the length, age and complexity of the file, but regardless, any review would consume a substantial amount of time.

**(U//LES)** [redacted]

20. (U//LES) [redacted]

[redacted]

21. (U//LES) [redacted]

[redacted]

22. (U//LES) [redacted]

23. (U) The analyst would next conduct a review of all FBI holdings. This involves a review of any and all documents, called serials, housed in various FBI databases. These databases may contain summaries of a reporting or source document with an attachment providing further

information on the particular topic or individual discussed. Older case files may not be readily accessible. The case files may pre-date electronic filing or storage for example and thus the information may not be stored on an FBI database. A special hand file search would be required in these instances and could be quite lengthy and time consuming. The process would involve identifying the physical records, determining where the records are located and stored, and conducting a complete review of the records to identify any relevant documents or information. These source documents, including databases and paper based records, are typically classified and information stored therein is compartmentalized, subject to numerous dissemination and access controls. For sensitive cases, only the case agent and his immediate case team have access to the information. A TSC analyst would therefore have to request from and coordinate with the case agent to access the information in question.

**(U//LES)** [redacted]

24. (U) Given the complexity and multiplicity of variables which could contribute to a record review, it is not possible for the TSC to make a precise estimate of how long it would take to conduct a review of an average TSDB record. Accordingly, I will utilize an artificial baseline estimate of **one hour** per record to complete a comprehensive review of that individual TSDB record - for which the basis is theoretical as no such review of this scale or

type has been previously attempted - taking into account each of the aforementioned factors, including the size and complexity of the record, how many of aforementioned steps (including duration and involvement of each step) and how many limitations are encountered (existence of source material, access to source material, etc.). Uncomplicated records with minimal information, few versions, and easily accessible underlying derogatory information could be reviewed in much less time. Conversely, some record reviews could take several hours or days, depending on complexity, impediments and limitations. This estimate shows that a competent, thorough and accurate completion of the searches requested in Plaintiff's interrogatories would levy an unreasonable burden on the Government. Significantly, there is also a distinct possibility that after exhausting all review resources, an analyst may not find responsive information at all. For instance, after a comprehensive review of the underlying source information, information that would lead to a conclusion or reasonable inference regarding, for example, religious affiliation, place of birth, etc., may not exist.

25. (U//LES) [redacted]

[redacted]

26. (U//LES) [redacted]

[redacted]

## (U) THE BURDEN ASSOCIATED WITH THE TYPES OF INFORMATION SOUGHT BY PLAINTIFF

27. (U//LES/SSI) [redacted]

[redacted]

28. (U//LES/SSI) [redacted]

[redacted]

[redacted]

29. (U//LES/SSI) [redacted]

30. (U) Further, even if such a burdensome search for information were conducted, it may not yield complete, accurate, or reliable information. First, if the field is completed, the TSC could conduct a search for specific terms but, because the field is free-form, the results may vary depending upon how the information was entered over time into the TSDB (e.g., New York City, NY, United States, US, USA). Second, even if any such information could be provided, the information does not provide an accurate, overall picture of the places of birth of U.S. persons on the No Fly List. For example, as of May 2014, only 26% of persons in the TSDB have a populated "place of birth" field, and this includes persons for whom multiple places of birth are listed. Third, any data entered into the place of birth field would be based on the reporting from the underlying records. The reporting on the underlying record itself may not be accurate or verifiable. The individual may have provided fraudulent information (e.g., in an immigration or visa application) or self-reported a place of birth that is not the person's actual place of birth, thus the information in the record is inaccurate, but still part of the individual's underlying record.

31. (U) *Searches for citizenship information.* Several of the interrogatories—Interrogatories 4, 7, 8, and 10—seek information about or based upon the U.S. citizenship status of persons in the TSDB or on the No Fly List. The manner by which the TSDB records citizenship status

has changed over the years. As discussed in the interrogatory responses, the TSDB does not track individuals as U.S. citizens. From 2003 through 2008, the TSDB did not track U.S. citizenship status. In 2008, the TSDB began tracking individuals as USPERs, which, as defined by Executive Order 12,333, includes both U.S. citizens and permanent resident aliens. Beginning on May 18, 2012, the TSDB also began tracking the lawful permanent resident (LPR) status of individuals; however, it did so only for individuals newly added to the TSDB. In other words, for individuals in the TSDB prior to May 18, 2012, the TSDB did not track them by LPR status but rather only as a USPER or non-USPER. Additionally, there are instances in which information about whether an individual is an USPER or non-USPER (since 2008), or as an LPR or non-LPR (since 2012), is not verified but rather is presumed based upon other facts. There are also instances in which the information regarding the USPER or LPR status that is used for identifying purposes may be fraudulent.

32. (U) In light of the way in which the TSDB has tracked U.S. citizenship status over the years, Defendants have answered these interrogatories to the extent possible based on available USPER data after 2009.

33. (U//LES/SSI) [redacted]

[redacted]

[redacted]

34. (U//LES/SSI) [redacted]

[redacted]

[redacted]

35. (U) With regard to Plaintiff's request for information about rejected nominations (Interrogatories 6 and 18), as explained in the interrogatory responses, the TSC does not, in the usual course of business, track or aggregate the basis for the rejection of a nomination for inclusion in the TSDB. When a nomination for inclusion in the TSDB is rejected, TSC records require only that a rejected nomination be identified as having insufficient "minimum criteria." TSC personnel reviewing a nomination are able to provide additional details about the basis for the rejection of a nomination in a free-form part of the record. However, because of the free form nature of this field, text provided may, may not, or may only partially address the basis for the rejection. Therefore, any purported statement about the basis for a rejection cannot be considered to represent the full or complete actual basis for the

decision. The current version of TSDB stores a free-form/text reject comment field that may be used to label the reject reason (as described in paragraph 15, above). The TSC SOP (Standard Operating Procedure) requires some form of (unclassified) *content* in the comments field of all rejected nominations. The content does not require that the *reason* for the rejection be specified. This comment-but-not-reason requirement has always been standard procedure. Additionally, because the field is free-form/text, there is no uniform comment structure nor required level of detail regarding the particular reason(s) for the nomination rejection, thus there are potential inconsistencies in that documentation. As noted previously, TSC identifies an "add" nomination as an initial request to watchlist a new individual. Presently (under current TSC SOP), during the add nomination review process, a record may be rejected for one or more of the following reasons:

a) (U) Lack of Minimum Identifying Criteria (MIC): the nomination does not contain sufficient identifying information to warrant inclusion in TSDB and supported systems;

b) (U) Lack of Minimum Substantive Derogatory Criteria (MSDC): the nomination does not contain sufficient derogatory information to warrant inclusion in TSDB and supported systems;

c) (U) System/Business Rule: nomination failed TSDB system and/or business rules set-up to ensure proper entry of nominations (e.g., duplicate nominations already received by TSDB and nominations lacking a name).

36. (U) TSC's Data Management Team (DMT) has identified approximately 13,244 TSDB record rejections since 2009 (with an additional 939 records deleted through system/business rule computer automated action). A manual review of the record of a rejected nomination to determine the reason for a rejection should not typically be as time-consuming as the comprehensive evaluation associated with the review of an entire TSDB record. However, assuming a theoretical baseline of approximately **15 minutes** per record (with similar considerations described in paragraph 24 above, including record complexity and availability of information), and also based on the assumption that TSC would only view its internal records and not seek out any underlying source documents, such a review would consume approximately 3,546 analyst-hours. At that rate, in order to complete the review of 13,244 records within 6 months, four (4) senior analysts would be needed and staffed full-time (to the exclusion of any and all other operational activity) to complete the project. Such a burdensome search would be compounded should a review and analysis of underlying source documents be required.

37. (U) A further complication exists, however. The standards for watchlisting placement and the standard operating procedures (SOP) associated with nominations have changed over the years. Therefore, any search or review of information regarding the basis for a rejected nomination would have to be assessed based upon the watchlistng standards and operating procedures that were in effect as of the time of the nomination. For standards that have not been in effect for a long period of time, analysis and review of such records would require additional time because an analyst would have to apply outdated and (currently) unused watchlisting standards and operating procedures simply to conduct a competent review of the underlying information on those older records to determine if responsive information exists. Analysts would be required to undergo training to achieve familiarity with each of the applicable prior watchlisting policies and guidance and remember to apply the appropriate ones to the affected records for the particular time period in question to accurately attempt to recreate the environmental factors that existed at the time.

**SUMMARY OF ESTIMATED TIME TO CONDUCT REVIEW SOUGHT BY PLAINTIFF**

38. (U//LES/SSI) [redacted]

[redacted]

~~UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE~~
~~SENSITIVE SECURITY INFORMATION~~

Pursuant to 28 U.S.C. §1746, I declare under penalty of perjury that the foregoing is true and correct.
Executed this 27 day of May, 2014, in Vienna, Virginia.

G. Clayton Grigg
Deputy Director for Operations
Terrorist Screening Center



~~UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE~~
~~SENSITIVE SECURITY INFORMATION~~