IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF CALIFORNIA

(HONORABLE JEFFREY T. MILLER)

UNITED STATES OF AMERICA, Plaintiff v. BASAALY SAEED MOALIN, MOHAMED MOHAMED MOHAMUD, ISSA DOREH, and AHMED NASIR TAALIL MOHAMUD, Defendants.	)	No. 10-CR-4246-JM

GOVERNMENT'S UNCLASSIFIED MEMORANDUM IN OPPOSITION TO DEFENDANT'S MOTION TO SUPPRESS INTERCEPTIONS MADE PURSUANT TO FISA AND ANY FRUITS THEREOF AND/OR FOR DISCLOSURE OF THE UNDERLYING FISA APPLICATIONS

I. INTRODUCTION

The Government files this unclassified, redacted memorandum in opposition to Basaaly Saeed Moalin's ("Moalin" or "the defendant") Motion to Suppress All Interceptions Made Pursuant to the Foreign Intelligence Surveillance Act and Any Fruits Thereof, and/or for Disclosure of the Underlying Applications for FISA Warrants ("defendant's motion") (Docket No. 92).[1] Defendant's motion seeks: (1) the Court's review of all of the relevant applications under the Foreign Intelligence Surveillance Act, as amended ("FISA");[2] (2) disclosure of such applications, orders and related materials (collectively "the FISA materials"); (3) a hearing under *Franks v. Delaware*, 438 U.S. 154 (1978); and (4) the suppression of information obtained or derived from FISA. Defendant's motion has triggered this Court's review of the FISA applications and orders pursuant to 50 U.S.C. §§ 1806(f) and 1825(g) to conduct an *ex parte* and *in camera* review to determine whether the FISC-authorized electronic surveillance and/or physical searches[3] of Moalin and Mohamud Abdi Yusuf ("Yusuf") were lawfully authorized and conducted.

---

[1] On December 12, 2011, Moalin's co-defendant, Issa Doreh ("Doreh"), moved to join motions made by his co-defendants to the extent "they inure to his benefit." (Docket No. 104). On December 15, 2011, Moalin's co-defendant, Mohamed Mohamed Mohamud ("Mohamud"), filed a similar motion to join (Docket No. 106). These motions to join do not present any additional grounds or arguments.

[2] **[CLASSIFIED MATERIAL REDACTED]**

[3] **[CLASSIFIED MATERIAL REDACTED]**

[CLASSIFIED MATERIAL REDACTED][4]

A. BACKGROUND

On October 22, 2010, a federal grand jury sitting in the Southern District of California returned an indictment against defendants Moalin, Mohamud, and Doreh (Docket No. 1). These defendants were charged with Conspiracy to Provide Material Support to Terrorists, in violation of 18 U.S.C. § 2339A (Count 1); Conspiracy to Provide Material Support to a Foreign Terrorist Organization, in violation of 18 U.S.C. § 2339B (Count 2); Conspiracy to Kill in a Foreign Country, in violation of 18 U.S.C. § 956 (Count 3); and Conspiracy to Launder Monetary Instruments, in violation of 18 U.S.C. § 1956 (Count 4). The indictment also charged defendant Moalin with one count of Providing Material Support to Terrorists, in violation of 18 U.S.C. § 2339A (Count 5). On January 14, 2011, the grand jury returned a Superseding Indictment including the same counts, but adding defendant Ahmed Nasir Taalil Mohamud ("Nasir") on Counts 1 through 4 (Docket No. 38). All defendants are charged in connection with providing money and support to the Somali-based designated foreign terrorist organization, Harakat Al Shabaab Al-Mujahedin ("Al-Shabaab").

On February 26, 2008, the United States Department of State formally designated Al-Shabaab as a Foreign Terrorist Organization under Section 219 of the Immigration and Nationality Act, as amended, and as a Specially Designated Global Terrorist under Section 1(b) of Executive Order 13224, as amended. Al-Shabaab is a violent and brutal militia group that uses

---

[4] **[CLASSIFIED MATERIAL REDACTED]**

intimidation and violence to undermine Somalia's Transitional Federal Government ("TFG") and its supporters. The superseding indictment charges, among other things, that the defendants conspired to provide material support to Al-Shabaab by soliciting, collecting, and transferring money from the United States to Aden Hashi Ayrow ("Ayrow") who, until his death by missile strike on May 1, 2008, was an Al-Shabaab leader. Moalin also provided Ayrow with the use of one of Moalin's properties in Somalia, and explained to him how he could hide weapons in the attic or yard. After Ayrow was killed, the defendants continued to collect funds and transmit them to Somalia to support violence against the TFG and its supporters.[5]

[CLASSIFIED MATERIAL REDACTED][6]

On November 4, 2010, the Government provided written notice to the Court and to Moalin, Mohamud, and Doreh pursuant to FISA that, at trial, the Government intends to use information obtained or derived from electronic surveillance conducted under the Foreign Intelligence Surveillance Act. (Docket No. 12.) On January 21, 2011, Nasir was provided with similar notice. (Docket No. 44.) On January 30, 2012, the Government provided written notice to

---

[5] This overview is not intended to be a comprehensive catalog of the defendants' actions, nor of the intended uses of the funds transferred to Somalia, which are the subject of the superseding indictment.

[6] **[CLASSIFIED MATERIAL REDACTED]**

Under FISA, "Attorney General" means the Attorney General of the United States (or Acting Attorney General), the Deputy Attorney General, or, upon the designation of the Attorney General, the Assistant Attorney General designated as the Assistant Attorney General for National Security. *See* 50 U.S.C. § 1801(g).

all four defendants of its intent to use information obtained or derived from physical search conducted under the Foreign Intelligence Surveillance Act. (Docket No. 119.)

[CLASSIFIED MATERIAL REDACTED][7] [8]

The Government's pleadings and the supporting FISA materials are submitted not only to oppose the defendant's motion, but also to support the Government's request, pursuant to FISA, that this Court: (1) conduct an *in camera, ex parte* review of the FISA materials; (2) find that the FISA collection at issue was both lawfully authorized and lawfully conducted; and (3) order that none of the classified documents, nor any of the classified information contained therein, be disclosed to the defense, and instead, that they be maintained under seal.

---

[7] As a result of the redactions, the pagination and footnote numbering of the classified memorandum and the unclassified memorandum are different.

[8] **[CLASSIFIED MATERIAL REDACTED]**

B. OVERVIEW OF THE FISA COLLECTION AT ISSUE

[CLASSIFIED MATERIAL REDACTED][9] [10] [11] [12] [13] [14] [15] [16] [17]

II. THE FISA PROCESS

A. OVERVIEW OF FISA

Enacted in 1978, and subsequently amended, FISA authorizes the Chief Justice of the United States to designate eleven United States District Judges to sit as judges of the FISC. 50 U.S.C. § 1803(a)(1). The FISC judges are empowered to consider *ex parte* applications submitted by the Executive Branch for electronic surveillance and physical searches when a significant purpose of the application is to obtain foreign intelligence information, as defined in FISA. Rulings of the FISC are subject to review by the Foreign Intelligence Surveillance Court of Review ("FISC of Review"), which is composed of three United States District Court or Circuit

---

[9] **[CLASSIFIED MATERIAL REDACTED]**

[10] **[CLASSIFIED MATERIAL REDACTED]**

[11] **[CLASSIFIED MATERIAL REDACTED]**

[12] **[CLASSIFIED MATERIAL REDACTED]**

[13] **[CLASSIFIED MATERIAL REDACTED]**

[14] **[CLASSIFIED MATERIAL REDACTED]**

[15] **[CLASSIFIED MATERIAL REDACTED]**

[16] **[CLASSIFIED MATERIAL REDACTED]**

[17] **[CLASSIFIED MATERIAL REDACTED]**

Judges who are designated by the Chief Justice. 50 U.S.C. § 1803(b). As discussed below, a District Court also has jurisdiction to determine the legality of electronic surveillance and physical searches authorized by the FISC when the fruits of that intelligence collection are used against an "aggrieved person."[18] *See* 50 U.S.C. §§ 1806(f), 1825(g).

As originally enacted, FISA required that a high-ranking member of the Executive Branch of Government certify that "the purpose" of the FISA application was to obtain foreign intelligence information. In 2001, FISA was amended as part of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act).[19] As discussed in more detail, *infra* pages 32 through 36, the pre-USA PATRIOT Act FISA language required that the Government certify that "the purpose" of the surveillance was the acquisition of foreign intelligence information, which was interpreted to mean "the primary purpose." The USA PATRIOT Act eliminated the requirement that the primary purpose of the requested FISA surveillance be the gathering of foreign intelligence information; instead, a high-ranking official is now to certify that the acquisition of foreign

---

[18] An "aggrieved person" is defined as the target of electronic surveillance or "any other person whose communications or activities were subject to electronic surveillance," 50 U.S.C. § 1801(k), as well as "a person whose premises, property, information, or material is the target of physical search" or "whose premises, property, information, or material was subject to physical search. 50 U.S.C. § 1821(2). Each of the defendants is an "aggrieved person" under FISA, and as noted above, they were provided with notice of their status as such and of the Government's intent to use FISA-obtained or -derived information against them at trial.

[19] Pub. L. No. 107-56, 115 Stat. 271 (2001).

intelligence information is "a significant purpose" of the requested surveillance. 18 U.S.C. § 1804(a)(6)(B).

At the time of the emergency authorizations here, FISA provided that in emergency situations the Attorney General may authorize electronic surveillance and physical search without an order from the FISC. *See* 50 U.S.C. §§ 1805(e), 1805(f), 1824(e) (effective March 9, 2006, to July 9, 2008). Before doing so, the Attorney General had to reasonably determine that "an emergency situation exists" that requires the employment of electronic surveillance or physical search to obtain foreign intelligence information before a FISC order could be obtained, and that the factual basis that would support a FISC order authorizing electronic surveillance or physical search exists. 50 U.S.C. §§ 1805(f)(1)-(2), 1824(e)(1)(B) (effective March 9, 2006, to July 9, 2008); *Global Relief Foundation v. O'Neill*, 207 F. Supp. 2d 779, 790 (N.D. Ill. 2002). The Attorney General also was required to inform the judge of the FISC having jurisdiction at the time the emergency authorization was granted, and apply for a FISC order authorizing the electronic surveillance or physical search "as soon as practicable," but not later than 72 hours after the emergency authorization. 50 U.S.C. §§ 1805(f), 1824(e)(1)(A) (effective March 9, 2006, to July 9, 2008). Emergency electronic surveillance or physical search had to comport with FISA's

minimization requirements, discussed below. *See* 50 U.S.C. §§ 1805(f), 1824(e)(2) (effective March 9, 2006, to July 9, 2008).[20]

B. THE FISA APPLICATION

FISA provides a statutory procedure whereby the Executive Branch may obtain a judicial order or warrant authorizing the use of electronic surveillance and/or physical searches within the United States where a significant purpose is the collection of foreign intelligence information. 50 U.S.C. §§ 1804(a)(6)(B), 1823(a)(6)(B); *see also United States v. Abu-Jihaad*, 630 F.3d 102, 117-118 (2d Cir. 2010); *United States v. Johnson*, 952 F.2d 565, 571-72 (1st Cir. 1992). Under FISA, "[f]oreign intelligence information" includes information that "relates to, and if concerning a United States person[21] is necessary to, the ability of the United States to protect against . . . actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power

---

[20] As it relates to emergency authorizations, the current version of FISA is largely identical to the version at issue in this case; the primary difference is that FISA now permits the Government up to seven days before it must apply for an order from the FISC.

If no FISC order authorizing the electronic surveillance or physical search is issued, emergency surveillance must stop when the information sought is obtained, when the FISC denies an application for an order, or after the expiration of 72 hours from the time of the emergency authorization, whichever is earliest. *See* 50 U.S.C. §§ 1805(f), 1824(e)(3) (effective March 9, 2006, to July 9, 2008). In addition, if no FISC order is issued, neither information obtained nor evidence derived from the emergency electronic surveillance or physical search may be disclosed in any court or other proceeding, and no information concerning a United States person acquired from the electronic surveillance or physical search may be used in any other manner by federal officers or employees without the person's consent, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm. *See* 50 U.S.C. §§ 1805(f), 1824(e)(4) (effective March 9, 2006, to July 9, 2008).

[21] **[CLASSIFIED MATERIAL REDACTED]**

[and/or] sabotage or international terrorism by a foreign power or an agent of a foreign power." 50 U.S.C. §§ 1801(e), 1821(1). "Foreign intelligence information" also includes information with respect to a "foreign power or foreign territory that relates to, and if concerning a United States person is necessary to – (A) the national defense or the security of the United States; or (B) the conduct of the foreign affairs of the United States." 50 U.S.C. §§ 1801(e)(2), 1821(1). With the exception of emergency authorizations, FISA requires that a court order be obtained before any electronic surveillance or physical search may be conducted.[22]

An application to conduct electronic surveillance pursuant to FISA must contain, among other things: (1) the identity of the federal officer making the application; (2) the identity, if known, or a description of the specific target of the electronic surveillance; (3) a statement of the facts and circumstances supporting probable cause to believe that the target is a foreign power or an agent of a foreign power, and that each facility or place at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;[23] (4) a statement of the proposed minimization procedures to be followed; (5) a detailed description of the nature of the information sought and the type of communications or activities to be

---

[22] **[CLASSIFIED MATERIAL REDACTED]**

[23] Moalin erroneously states that "FISA appears to require that both the information sought *and* the communications subject to surveillance would have to relate directly to activities involving both an agent of foreign power and international terrorism as defined in FISA." (Docket No. 92 at 10-11). In fact, FISA does not require an application for electronic surveillance demonstrate a relationship between the type of information sought and the communications subject to

subjected to the surveillance; (6) a certification, discussed below, of a high-ranking official; (7) the manner or means by which the electronic surveillance or physical search will be effected and a statement whether physical entry is required to effect the electronic surveillance; (8) the facts concerning and the action taken on all previous FISA applications involving any of the persons, facilities, places, premises or property specified in the application; and (9) the proposed duration of the electronic surveillance or physical search. *See* 50 U.S.C. § 1804(a)(1)-(9).

An application to conduct a physical search pursuant to FISA must contain similar information as an application to conduct electronic surveillance. *See* 50 U.S.C. § 1823(a)(1)-(8). The primary difference is that an application to conduct a physical search must also contain a statement of the facts and circumstances establishing probable cause that "each premises or property to be searched is owned, used, possessed by, or is in transit to or from" the target. *See* 50 U.S.C. § 1823(a)(3)(C).[24]

---

surveillance. *See* 50 U.S.C. § 1805(a)(2)(B)(application must show facilities to be monitored are being used, or about to be used, by agent of a foreign power).

[24] An application to conduct a physical search must also contain a statement of the facts and circumstances justifying the belief that "the premises or property to be searched contains foreign intelligence information." 50 U.S.C. § 1823(a)(3)(B).

1. The Certification

An application to the FISC for a FISA order or warrant[25] must include a certification from a high-ranking Executive Branch official with national security responsibilities that:

> (A) the certifying official deems the information sought to be foreign intelligence information;
>
> (B) a significant purpose of the surveillance is to obtain foreign intelligence information;
>
> (C) such information cannot reasonably be obtained by normal investigative techniques;
>
> (D) designates the type of foreign intelligence information being sought according to the categories described in 50 U.S.C. § 1801(e); and
>
> (E) includes a statement of the basis for the certification that –
>
> > (i) the information sought is the type of foreign intelligence information designated; and
> >
> > (ii) such information cannot reasonably be obtained by normal investigative techniques.

50 U.S.C. § 1804(a). *See also* 50 U.S.C. § 1823(a) (physical search).

---

[25] **[CLASSIFIED MATERIAL REDACTED]**

2. Minimization Procedures

The Attorney General has adopted, and the FISC has approved, minimization procedures that regulate the acquisition, retention, and dissemination of information obtained through FISA collection about United States persons, including persons who are not the FISA targets of the FISA collection. FISA requires that such minimization procedures be:

> reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.

50 U.S.C. § 1801(h)(1); *see also* 50 U.S.C. § 1821(4)(A) (physical search).

In addition, minimization procedures also include "procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes." 50 U.S.C. § 1801(h)(3); *see also* 50 U.S.C. § 1821(4)(c) (physical search).

In order to fulfill the statutory requirements discussed above, the Attorney General has adopted standard minimization procedures for FISC-authorized electronic surveillance and physical search that are on file with the FISC and that are incorporated by reference into every relevant FISA application that is submitted to the FISC. As a result, the eight FISC judges who issued the orders authorizing the FISA collections at issue in this case found that the applicable standard minimization procedures met FISA's statutory requirements. The FISC orders in the dockets at issue directed the Government to follow the approved minimization procedures in conducting the FISA collection.

3. Attorney General's Approval

FISA further requires that the Attorney General[26] approve applications for electronic surveillance and/or physical search before they are presented to the FISC.

C. THE FISC'S ORDERS

Once approved by the Attorney General, the application is submitted to the FISC and assigned to one of its judges. The FISC may approve the requested electronic surveillance or physical search only upon finding, among other things, that: (1) the application has been made by a "Federal officer" and has been approved by the Attorney General; (2) there is probable cause to believe that (a) the target of the electronic surveillance and/or physical search is a foreign power or an agent of a foreign power, and that (b) the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power and/or that the premises or property to be searched is owned, used, possessed by, or is in transit to or from a foreign power or an agent of a foreign power; (3) the proposed minimization procedures meet the statutory requirements set forth in 50 U.S.C. § 1801(h) (electronic surveillance) and/or 50 U.S.C. § 1821(4) (physical search); (4) the application contains all of the statements and certifications required by Section 1804 or Section 1823; and (5) if the

---

[26] As noted above, "Attorney General" means the Attorney General of the United States (or Acting Attorney General), the Deputy Attorney General, or, "upon . . . the designation of the Attorney General, the Assistant Attorney General designated as the Assistant Attorney General for National Security." *See* 50 U.S.C. § 1801(g).

target is a United States person, that the certifications are not clearly erroneous. 50 U.S.C. §§ 1805(a)(1)-(4), 1824(a)(1)-(4).

FISA defines "foreign power" to include "a group engaged in international terrorism or activities in preparation therefor," 50 U.S.C. §§ 1801(a)(4), 1821(1). As it relates to United States persons, "agent of a foreign power" includes any person who:

> (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;
>
> * * * * * * *
>
> or
>
> (E) knowingly aids or abets any person in the conduct of activities described in [the subparagraphs above] . . . or knowingly conspires with any person to engage in activities described in [the subparagraphs above.]

50 U.S.C. §§ 1801(b)(2) (electronic surveillance), 1821(1) (physical search).

FISA specifies that no United States person may be considered a foreign power or an agent of a foreign power *solely* on the basis of activities protected by the First Amendment to the Constitution of the United States. 50 U.S.C. §§ 1805(a)(2)(A), 1824(a)(2)(A) (emphasis added). This means that while protected First Amendment activities cannot form the sole basis for FISC-authorized electronic surveillance or physical search, they may be considered by the FISC if there is other activity indicative that the target is an agent of a foreign power. *United States v. Rosen*, 447 F. Supp. 2d 538, 549-50 (E.D. Va. 2006); *United States v. Rahman*, 861 F. Supp. 247, 252 (S.D.N.Y. 1994), *aff'd*, 189 F.3d 88 (2d Cir. 1999). Additionally, FISA provides that "[i]n determining whether or not probable cause exists . . . a judge may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target." 50 U.S.C. §§ 1805(b), 1824(b).

If the FISC is satisfied that the FISA application meets the statutory provisions and has made all of the necessary findings, the FISC issues an *ex parte* order authorizing the electronic surveillance and/or physical search requested in the application. 50 U.S.C. §§ 1805(a), 1824(a). The order must specify: (1) the identity (or a description of) the specific target of the collection; (2) the nature and location of each facility or place at which the electronic surveillance will be directed or of each of the premises or properties that will be searched; (3) the type of information sought to be acquired and the type of communications or activities that are to be subjected to the electronic surveillance, or the type of information, material, or property that is to be seized, altered, or reproduced through the physical search; (4) the means by which electronic surveillance will be effected and whether physical entry will be necessary to effect that surveillance, or a statement of the manner in which the physical search will be conducted; (5) the period of time during which electronic surveillance is approved and/or the authorized scope of each physical search; and (6) the applicable minimization procedures. 50 U.S.C. §§ 1805(c)(1), 1824(c)(1). The FISC also retains the authority to review, before the end of the authorized period of electronic surveillance or physical search, the United States' compliance with the requisite minimization procedures. 50 U.S.C. §§ 1805(d)(3), 1824(d)(3).

Under FISA, electronic surveillance and/or physical searches targeting a United States person may be approved for up to ninety days. 50 U.S.C. §§ 1805(d)(1), 1824(d)(1). Extensions may be granted, but only if the United States submits another application that complies with FISA's requirements. 50 U.S.C. §§ 1805(e)(2), 1824(d)(2).

III. DISTRICT COURT REVIEW OF FISC ORDERS

FISA authorizes the use in a criminal prosecution of information obtained or derived

from any FISC-authorized electronic surveillance and/or physical search, provided that advance authorization is obtained from the Attorney General, *see* 50 U.S.C. §§ 1806(b), 1825(c), and that proper notice is given to the court and to each aggrieved person against whom the information is to be used, *see* 50 U.S.C. §§ 1806(c), (d), and 1825(d), (e). Upon receiving notice, an aggrieved person may then move to suppress the use of the FISA information on two grounds: (1) that the information was unlawfully acquired under FISA; or (2) that the electronic surveillance or physical search was not conducted in conformity with the FISC's order(s). 50 U.S.C. §§ 1806(e), 1825(f). Accordingly, as discussed in detail in later sections, disclosure and suppression motions are evaluated using FISA's probable cause standard, not the probable cause standard for criminal warrants. *See, e.g.*, *United States v. El-Mezain*, 664 F.3d 467, 564 (5th Cir. 2011) ("This probable cause standard is different from the standard in the typical criminal case because, rather than focusing on probable cause to believe that a person has committed a crime, the FISA standard focuses on the status of the target as a foreign power or an agent of a foreign power."); *United States v. Duka*, __ F.3d ___, No. 07-CR-00459, 2011 WL 6794022, at *4 (3d Cir. 2011) (rejecting appellant's challenge to FISA's probable cause standard because it does not require indications that a crime has been committed); *United States v. Pelton*, 835 F.2d 1067, 1075 (4th Cir. 1987).

A. THE REVIEW IS TO BE CONDUCTED *IN CAMERA* AND *EX PARTE*

In assessing the legality of challenged FISA electronic surveillance or physical searches, the district court "shall, notwithstanding any other law, if the Attorney General files [as he has filed in this proceeding] an affidavit or declaration under oath that disclosure or an adversary hearing would harm the national security of the United States, review *in camera* and *ex parte* the

application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted." 50 U.S.C. §§ 1806(f), 1825(g).[27] If, after conducting its *in camera* and *ex parte* review, the court determines that it is unable to make an accurate determination of the legality of the collection, the court "may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order or other materials relating to the surveillance [or physical search] *only where such disclosure is necessary* to make an accurate determination of the legality of the surveillance [or search]." 50 U.S.C. §§ 1806(f), 1825(g) (emphasis added). Thus, the propriety of the disclosure of any FISA applications or orders to the defendant cannot even be considered unless and until the district court has first concluded that it is unable to make an accurate determination of the legality of the collection after reviewing the Government's submissions (and any supplemental pleadings that the district court may request) *in camera* and *ex parte*. *See El-Mezain*, 664 F.3d at 566; *Abu-Jihaad*, 630 F.3d at 129; *United States v. Belfield*, 692 F.2d 141, 147 (D.C. Cir. 1982); *United States v. Kashmiri*, No. 09-CR-830-4, 2010 WL 4705159, at *2 (N.D. Ill., November 10, 2010); *United States v. Nicholson*, Case No. 09-CR-40, 2010 WL 1641167, at *4 (D. Or. April 21, 2010) ("After an *in-camera* review, the court 'has the discretion to disclose portions of the documents, under appropriate protective orders, *only if [the court] decides that such disclosure is necessary to make an accurate*

---

[27] The defendant concedes that 50 U.S.C. § 1806(f) requires an *in camera* review, but omits the "*ex parte*" requirement. Docket No. 92 at 13.

determination of the legality of the surveillance.'") (quoting *United States v. Duggan*, 743 F.2d 59, 78 (2d Cir. 1984) (emphasis in *Nicholson*); *United States v. Islamic American Relief Agency ("IARA")*, No. 07-CR-00087, 2009 WL 5169536, at *3-4 (W.D. Mo. December 21, 2009).

If the district court is able to make an accurate determination of the legality of the surveillance based on its *in camera, ex parte* review of the materials submitted by the United States, then the court *may not* order disclosure of any of the FISA materials to the defense, unless otherwise required by due process. *See* 50 U.S.C. § 1806(g); *El-Mezain*, 664 F.3d, at 566; *Duggan*, 743 F.2d, at 78; *Kashmiri*, 2010 WL 4705159, at *2.

1. *In Camera, Ex Parte* Review is the Rule

Federal courts have repeatedly and consistently held that FISA "anticipates that an *ex parte, in camera* determination is to be the rule," with disclosure and an adversarial hearing being the "exception, occurring *only* when necessary." *Belfield*, 692 F.2d at 147 (emphasis in original); *accord*, *El-Mezain*, 664 F.3d, at 567 ("[D]isclosure of FISA materials is the exception and *ex parte, in camera* determination is the rule.") (citing *Abu Jihaad*, 630 F.3d at 129); *Duggan*, 743 F.2d at 78; *Rosen*, 447 F. Supp. 2d at 546; *Nicholson*, 2010 WL 1641167 at *3-4; *United States v. Spanjol*, 720 F. Supp. 55, 59 (E.D. Pa. 1989), *aff'd*, 958 F.2d 365 (3d Cir. 1992). Indeed, no court has *ever* found it necessary to disclose FISA materials to a criminal defendant to assist the court's determination of the lawfulness of either electronic surveillance or physical searches under FISA. *See El-Mezain*, 664 F.3d, at 566 (quoting the district court's statement that no court has ever ordered disclosure); *In re Grand Jury Proceedings of the Special April 2002 Grand Jury* ("*In re Grand Jury Proceedings*"), 347 F.3d 197, 203 (7th Cir. 2003) (noting that no court has ever ordered disclosure of FISA materials); *United States v. Mubayyid*, 521 F. Supp. 2d 125, 130 (D.

Mass. 2007) (collecting cases); *Rosen*, 447 F. Supp. 2d at 546 (same); *United States v. Gowadia*, No. 05-CR-00486, 2009 WL 1649714, at *2 (D. Haw. June 8, 2009); *Kashmiri*, 2010 WL 4705159, at *2. Indeed, to the Government's knowledge, no court has ever suppressed FISA-obtained or -derived information, or held an adversarial hearing on motions to disclose or to suppress.

In fact, every court that has addressed a motion to disclose FISA dockets or to suppress FISA materials has been able to determine the legality of the FISA collection at issue based on its *in camera, ex parte* review. *See, e.g.*, *Spanjol*, 720 F. Supp. at 58-59; *United States v. Sattar*, No. 02-CR-395, 2003 WL 22137012, at *6 (S.D.N.Y. 2003) (citing *United States v. Nicholson*, 955 F. Supp. 588, 592 & n. 11 (E.D.Va. 1997) ("this court knows of no instance in which a court has required an adversary hearing or disclosure in determining the legality of a FISA surveillance")), *aff'd*, 590 F.3d 93 (2d Cir. 2009); *see also El-Mezain*, 664 F.3d, at 566 (quoting district court's statement that no court has ever held an adversarial hearing to assist the court); *United States v. Thomson*, 752 F. Supp. 75, 79 (W.D.N.Y. 1990) (same); *United States v. Abu-Jihaad*, 531 F. Supp. 2d 299, 310 (D. Conn. 2008), *aff'd*, 630 F.3d 102, 129-30 (2d Cir. 2010); *Mubayyid*, 521 F. Supp. 2d at 130; *Rosen*, 447 F. Supp. 2d at 546; *United States v. Isa*, 923 F.2d 1300, 1305 (8th Cir. 1991).

There is nothing extraordinary about this case that would prompt the Court to be the first to order the disclosure of *highly* sensitive and classified FISA materials. Disclosure is not necessary for the Court to determine the legality of the collection. Here, the FISA dockets – at Sealed Exhibits 16-26 – are well-organized and easily reviewable by the Court *in camera* and *ex parte*. The *Index of Materials in the Government's Sealed Exhibit* and this memorandum serve as

a road map through the issues presented for the Court's *in camera* and *ex parte* determination. The FISA materials contain ample information from which the Court can make an accurate determination of the legality of the FISA collection; indeed, they are "relatively straightforward and not complex." *See, e.g., Abu-Jihaad*, 630 F. 3d at 129 (upholding district court's *in camera, ex parte* review where FISA materials were "relatively straightforward and not complex"); *In re Kevork*, 634 F. Supp. 1002, 1008 (C.D. Cal. 1985), *aff'd*, 788 F.2d 566 (9th Cir. 1986) (denying defendant's motion to disclose FISA materials where the materials were "straightforward and readily understood"); *Belfield*, 692 F.2d at 147 ("[t]he determination of legality in this case is not complex"); *United States v. Warsame*, 547 F.Supp.2d 982, 987 (D. Minn. 2008) (finding that "issues presented by the FISA applications are straightforward and uncontroversial"). Thus, there is no basis to disclose any of the FISA materials to the defendants. The Government respectfully submits that this Court, much like the aforementioned courts, is able to review the FISA dockets *in camera* and *ex parte*.

Defendant argues that disclosure is "necessary" in order for counsel to assist the Court in its determination that the surveillance and/or search was lawfully authorized and conducted. (Docket No. 92 at 24). However, disclosure of the FISA materials is not even an issue, let alone necessary, unless the "court's initial review indicates that the question of legality may be complicated" by factual misrepresentations, insufficient identification of the target, or failure to comply with the minimization standards in the order. *Warsame*, 547 F. Supp. 2d at 987 (*citing Belfield*, 692 F.2d at 147 (quoting S. Rep. No. 95-701, 95th Cong. 2d Sess. 64 (1978), *reprinted in* U.S. Code Cong. & Admin. News 3973, 4032-33). FISA mandates the Court must first find that

assistance from the defense is necessary and that finding is to be made *after* an *in camera, ex parte* review of the precise materials that the defense seeks to have disclosed *prior* to such review.

Moalin also argues that disclosure is appropriate because his attorneys hold security clearances. (Docket No. 92 at 24-25). But defendant predicates his argument on the Classified Information Procedures Act ("CIPA"),[28] which is inapplicable to the determination of a motion to disclose FISA materials. In short, whether a defense attorney possesses a security clearance is irrelevant to determining whether he or she is entitled to review FISA dockets. In *United States v. Ott*, 827 F.2d 473, 476-77 (9th Cir. 1987), the Ninth Circuit rejected defendant's security clearance argument, stating:

> [Defendant] next asserts that the *ex parte, in camera* proceeding violated due process in this case because his various attorneys all had high security clearances and therefore disclosure to them of the FISA materials would not entail or risk dissemination of sensitive information to non-cleared personnel. This argument is also unpersuasive. Congress has a legitimate interest in authorizing the Attorney General to invoke procedures designed to ensure that sensitive security information is not unnecessarily disseminated to *anyone* not involved in the surveillance operation in question, whether or not she happens for unrelated reasons to enjoy a security clearance. We reject the notion that a defendant's due process right to disclosure of FISA materials turns on the qualifications of his counsel.

Id. See also, e.g., Nicholson, 2010 WL 1641167, at *5 (referencing *Ott* and holding that "[b]ased on its *in-camera* review . . . the disclosure of FISA materials to [cleared] defense counsel is

---

[28] CIPA does not provide a basis for disclosure outside of the requirements of FISA. In fact, the opposite is true. These proceedings merely provide a process for protecting classified information in criminal discovery. Indeed, in CIPA proceedings *ex parte, in camera* consideration of the Government's applications for protective orders are the rule. *See, e.g., United States v. Klimavicius-Viloria*, 144 F.3d 1249, 1261 (9th Cir. 1998), (approving CIPA § 4 *ex parte* hearings); *United States v. Sarkissian*, 841 F.2d 959, 965-66 (9th Cir. 1998) (*ex parte* proceedings

neither required nor appropriate"); *United States v. Amawi*, No. 3:06-CR-719, 2009 WL 961143, at *2 (N.D. Ohio Apr. 7, 2009); *United States v. Bin Laden*, 126 F. Supp. 2d 264, 287 n. 26 (S.D.N.Y. 2000); *see also* Executive Order 13526, 32 C.F.R. 2001 (2003), *reprinted in* 75 Fed. Reg. 707, 720, 729 (Jan. 5, 2010) (requiring that a "need to know" determination be made prior to the disclosure of classified information to anyone, including those who possess a security clearance); *Badrawi v. Dep't of Homeland Security*, 596 F. Supp. 2d 389, 400 (D. Conn. 2009) (counsel held Top Secret security clearance but did not have a "need to know," and therefore was denied access to documents). Even cleared defense counsel have no "need to know" unless the Court determines that it cannot make an accurate determination of the legality of the FISA.

The Attorney General's Declaration sets forth that disclosure of the FISA materials would cause "exceptionally grave damage to the national security of the United States." *See* Sealed Exhibit 1, at ¶ 5. The specific harm that would result from the disclosure of the FISA dockets in this case is detailed in the classified declaration of FBI Assistant Director Ralph S. Boelter in support of the Attorney General's Declaration. *See* Sealed Exhibit 2. Moreover, the underlying rationale for non-disclosure is clear: "In the sensitive area of foreign intelligence gathering, the need for extreme caution and sometimes even secrecy may not be overemphasized." *Ott*, 827 F.2d, at 477 ("Congress has a legitimate interest in authorizing the Attorney General to invoke procedures designed to ensure that sensitive security information is not unnecessarily

---

concerning national security information are appropriate under CIPA § 4).

disseminated to anyone not involved in the surveillance operation in question."); *accord* IARA, 2009 WL 5169536, at *3-4.

Confidentiality is critical to national security. "If potentially valuable intelligence sources" believe that the United States "will be unable to maintain the confidentiality of its relationship to them, many [of those sources] could well refuse to supply information." *CIA v. Sims*, 471 U.S. 159, 175 (1985); *see also Phillippi v. CIA*, 655 F.2d 1325, 1332-33 (D.C. Cir. 1981). When a question is raised as to whether the disclosure of classified sources, methods, techniques, or information would harm the national security, federal courts have expressed a great reluctance to replace the considered judgment of Executive Branch officials charged with the responsibility of weighing a variety of subtle and complex factors in determining whether the disclosure of information may lead to an unacceptable risk of compromising the intelligence gathering process, and determining whether foreign agents, spies, and terrorists are capable of piecing together a mosaic of information that, when revealed, could reasonably be expected to harm the national security of the United States. *See Sims*, 471 U.S. at 180; *United States v. Yunis*, 867 F.2d 617, 623 (D.C. Cir. 1989) ("Things that did not make sense to the District Judge would make all too much sense to a foreign counter-intelligence specialist who could learn much about this nation's intelligence-gathering capabilities from what these documents revealed about sources and methods."); *Halperin v. CIA*, 629 F.2d 144, 150 (D.C. Cir. 1980) ("each individual piece of intelligence information, much like a piece of jigsaw puzzle, may aid in piecing together other bits of information even when the individual piece is not of obvious importance in itself"). An adversarial hearing is not only entirely unnecessary to aid the Court in the straightforward task

before it, but such a hearing would *create* potential dangers that courts have consistently sought to avoid.

As the *Belfield* court explained:

> Congress recognized the need for the Executive to engage in and employ the fruits of clandestine surveillance without being constantly hamstrung by disclosure requirements. The statute is meant to "reconcile national intelligence and counterintelligence needs with constitutional principles in a way that is consistent with both national security and individual rights." In FISA the privacy rights of individuals are ensured not through mandatory disclosure, but through its provisions for in-depth oversight of FISA surveillance by all three branches of government and by a statutory scheme that to a large degree centers on an expanded conception of minimization that differs from that which governs law enforcement surveillance.

692 F.2d at 148 (footnotes and citations omitted); *see also ACLU Foundation of So. Cal. v. Barr* ("*ACLU Foundation*"), 952 F.2d 457, 465 (D.C. Cir. 1991) (citing *Belfield* for the proposition that Section 1806(f) "is an acceptable means of adjudicating the constitutional rights of persons who have been subjected to FISA surveillance").

2. *In Camera, Ex Parte* Review is Constitutional

Moalin challenges the constitutionality of FISA's *ex parte*, *in camera* review procedures on due process grounds, attacking them as "antithetical to American criminal justice." (*See* Docket No. 92 at 25.) But he does not point to any decision involving a due process challenge to the FISA's *ex parte* and *in camera* review procedures.[29] Indeed, courts have universally rejected

---

[29] Moalin does not cite any case involving FISA. Instead, he relies upon a civil immigration case involving undisclosed, but not classified, material, and not involving FISA material, national

this position and found that FISA's *ex parte, in camera* review provisions satisfy the Due Process Clause of the Fifth Amendment. *See, e.g.*, *El-Mezain*, 664 F.3d at 566-67; *Abu Jihaad*, 630 F.3d at 129 (no violation of due process in district court's *in camera, ex parte* determination of FISA suppression motion); *United States v. Damrah*, 412 F.3d 618, 624 (6th Cir. 2005) ("FISA's requirement that the district court conduct an *ex parte, in camera* review of FISA materials does not deprive a defendant of due process."); *Gowadia*, 2009 WL 1649714, at *2; *United States v. Jayyousi*, No. 04-CR-60001, 2007 WL 851278, at *7 (S.D. Fla. Mar. 15, 2007), *aff'd*, 657 F.3d 1085 (11th Cir. 2011);[30] *United States v. Benkahla*, 437 F. Supp. 2d 541, 554 (E.D. Va. 2006); *ACLU Foundation*, 952 F.2d at 465; *United States v. Megahey*, 553 F. Supp. 1180, 1194 (E.D.N.Y. 1982) ("*ex parte*, *in camera* procedures provided in 50 U.S.C. § 1806(f) are constitutionally sufficient to determine the lawfulness of the electronic surveillance at issue while safeguarding defendants' fourth amendment rights"); *United States v. Falvey*, 540 F. Supp. 1306, 1315-16 (E.D.N.Y. 1982) (a "massive body of pre-FISA case law of the Supreme Court, [the Second] Circuit and others" supports the conclusion that the legality of electronic surveillance should be determined on an *in camera*, *ex parte* basis); *Belfield*, 692 F.2d at 148-49; *Nicholson*, 2010 WL 1641167, at *3-4.

---

security, or an Attorney General's Declaration and Claim of Privilege. *See* Docket No. 92 at 26 (*citing Am.-Arab Anti-Discrimination Comm. v. Reno*, 70 F.3d 1045, 1069 (9th Cir. 1995)).

[30] All citations to *Jayyousi* herein are to Westlaw because they are from a Magistrate Judge's Report and Recommendation that was adopted and incorporated into the Court's Opinion.

In summary, FISA mandates a process by which the district court must conduct an initial *in camera, ex parte* review of FISA applications, orders, and related materials in order to determine whether the FISA collection was lawfully authorized and lawfully conducted. Such *in camera, ex parte* review is the rule and is constitutional. In this case, the Attorney General has filed the required declaration invoking that procedure, and has declared that disclosure or an adversary hearing would harm national security.[31] (*See* Sealed Appendix at Ex. 1.) Accordingly, an *in camera, ex parte* review by this Court is the appropriate method by which to determine whether the FISA collection was lawfully authorized and conducted pursuant to FISA.

3. There is no Basis for a *Franks* Hearing

Moalin requests a *Franks* hearing and seeks disclosure of FISA materials for that purpose. (Docket No. 92 at 6-7, 19-20, 27). But he makes no effort to meet the standard for a *Franks* hearing. To merit an evidentiary hearing under *Franks*, the defendant must first make a "concrete and substantial preliminary showing" that: (1) the affiant deliberately or recklessly included false statements, or failed to include material information, in the affidavit; and (2) the misrepresentation was essential to the finding of probable cause. *Franks*, 438 U.S. at 155-56; *United States v. Colkley*, 899 F.2d 297, 301 (4th Cir. 1990); *Kashmiri*, 2010 WL 4705159, at * 6 (defendant "has not made any showing – let alone a substantial one – that an Executive Branch officer knowingly and intentionally, or recklessly, included a false statement in the FISA application [and w]ithout such a showing, he is foreclosed from obtaining a hearing"); *Duggan*, 743 F.2d at 77 n.6. Failure

---

[31] **[CLASSIFIED MATERIAL REDACTED]**

of the defendant "to satisfy either of these two prongs proves fatal to a *Franks* hearing." *Kashmiri*, 2010 WL 4705159, at * 5; *Mubayyid*, 521 F.Supp.2d at 130-31. The defendant's burden in establishing the need for a *Franks* hearing is a heavy one. *United States v. Jeffus*, 22 F.3d 554, 558 (4th Cir. 1994).

Furthermore, the defendant's lack of access to the FISA applications and orders does not eliminate the required showing. Although this situation presents a challenge to defendants, Congress and the courts have recognized that such difficulty does not justify disclosure of FISA materials:

> We appreciate the difficulties of appellants' counsel in this case. They must argue that the determination of legality is so complex that an adversary hearing with full access to relevant materials is necessary. But without access to relevant materials their claim of complexity can be given no concreteness. It is pure assertion.
>
> Congress was also aware of these difficulties. But it chose to resolve them through means other than mandatory disclosure. . . . Appellants are understandably reluctant to be excluded from the process whereby the legality of a surveillance by which they were incidentally affected is judged. But it cannot be said that this exclusion rises to the level of a constitutional violation.

Belfield, 692 F.2d at 148.

Similarly, in *Kashmiri,* 2010 U.S. Dist. LEXIS 119470, at * 17, the court rejected a *Franks* challenge in the context of a FISA suppression motion, and stated:

> [T]o challenge the veracity of the FISA application, Defendant must offer substantial proof that the FISC relied on an intentional or reckless misrepresentation by the government to grant the FISA order. The quest to satisfy the *Franks* requirement might feel like a wild-goose chase, as Defendant lacks access to the materials that would provide this proof. This perceived practical impossibility to obtain a hearing, however, does not constitute a legal impossibility.

Courts have routinely rejected defendants' attempts to force a *Franks* hearing challenging the validity of FISA orders. *See Abu-Jihaad*, 531 F. Supp. 2d at 311; *United States v. Hassoun*, 2007 WL 1068127, *4; *Mubayyid*, 521 F. Supp. 2d at 130-31; *Kashmiri*, 2010 WL 4705159, at *5-6 (noting that the court "has already undertaken a process akin to a *Franks* hearing through its *ex parte*, *in camera* review").

Moalin concedes there is no basis for a *Franks* hearing, stating he "cannot point to or identify any specific false statements or material omissions in [the FISA] applications" and that he cannot "[make] the showing that *Franks* ordinarily requires." (Docket No. 92 at 20.) Instead, he points to the "possibility that the government has submitted FISA applications with intentionally or recklessly false statements or material omissions" and observes that abuse of FISA authorities has occurred in the past in other instances. (Docket No. 92 at 20-21.) Nevertheless, "[t]he fact that the government has included misstatements and critical omissions in other FISA applications not at issue here cannot justify disclosure in this case." *Warsame*, 547 F. Supp. 2d at 987-88.

For all these reasons, the Court should deny the request for a *Franks* hearing.

4. There is No Basis for Disclosure of the FISA Materials Under FISA Section 1806(g)

Defendant also contends that Section 1806(g) of FISA provides an additional basis on which the Court might disclose the FISA materials to him. *See* Docket No. 92 at 25. Section 1806(g) does not support disclosure to the defendant. Section 1806(g) provides that "[i]f the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure." Defendant concedes that such disclosure is limited to discovery of exculpatory materials

mandated by *Brady* and its progeny. *See id.* at 25 (citing *Spanjol*, 720 F. Supp. at 57). A number of other courts have reached the same conclusion. *United States v. Amawi*, 531 F. Supp. 2d 832, 837 (N.D. Ohio 2008); *Abu-Jihaad*, 531 F. Supp. 2d at 311; *United States v. Thompson*, 752 F. Supp. 75, 82-83 (W.D.N.Y. 1990).[32] As the Court's *in camera, ex parte* review will demonstrate, there is no exculpatory information among the FISA materials; therefore, no disclosure is warranted pursuant to Section 1806(g).[33]

B. THE DISTRICT COURT'S SUBSTANTIVE REVIEW

1. Determination of Probable Cause - Standard of Review

Although federal courts are not in agreement as to whether the probable cause determinations of the FISC should be reviewed *de novo* or accorded deference, the materials under review would clear the higher standard of *de novo* review. *See Abu-Jihaad*, 630 F.3d at 130 ("Although the established standard of judicial review applicable to FISA warrants is deferential, the government's detailed and complete submission in this case would easily allow it to clear a higher standard of review."). The Government believes that it is appropriate to accord due deference to the findings of the FISC, but notes that a number of courts have declined to do so, and have instead reviewed the FISC's probable cause determinations *de novo*. *See, e.g., El Mezain*, 664 F.3d 467, 568 (5th Cir. 2011); *United States v. Hammoud*, 381 F.3d 316, 332 (4th

---

[32] As noted previously, no Court has ever ordered discovery of FISA materials. *See supra* at 24.

Cir. 2004), *rev'd on other grounds*, 543 U.S. 1097 (2005), *op. reinstated in pertinent part*, 405 F.3d 1034 (4th Cir. 2005).[34] Under either standard of review, the district court should determine: (1) whether the certifications submitted by the Executive Branch in support of the FISA application were properly made; (2) whether probable cause existed to authorize the electronic surveillance and/or physical search at issue; and (3) whether the collection was properly minimized. *See Abu-Jihaad*, 630 F.3d at 130-31.

With respect to emergency surveillance and/or physical searches, the district court's review should determine: (1) whether the FISC's order approving the emergency collection reasonably determined that "an emergency situation" and "the factual basis" for a FISC order authorizing collection existed "at the time the [collection] was conducted," *O'Neill*, 207 F. Supp. 2d at 790, and the Attorney General or a designee informed the FISC of the emergency collection; (2) whether the government properly applied for such approval "as soon as practicable" but not later than 72 hours after the emergency authorization; and (3) whether the collection was properly minimized. 50 U.S.C. §§ 1805(f), 1824(e) (effective March 9, 2006, to July 9, 2008).

---

[33] The government has complied with its *Brady* obligations with respect to the fruits of the FISA – the intercepted calls and fruits of the physical searches – and will continue to do so should it discover further exculpatory materials.

2. Certifications are Subject to only Minimal Scrutiny

Moalin urges this Court to subject the certifications supporting the FISA applications to "utmost scrutiny" and to review them "with particular care." (Docket No. at 22). However, he fails to cite a FISA case and instead relies upon *Blackmon v. United States*, 273 F.3d 1204, 1207 (9th Cir. 2001), which he acknowledges deals with Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"), 18 U.S.C. §§ 2510-2520 (1982). The Title III standard does not apply to FISA. Courts have unanimously agreed that certifications submitted in support of a FISA application should be "subjected to only minimal scrutiny by the courts," *Abu-Jihaad*, 630 F.3d at 120; *United States v. Badia*, 827 F.2d 1458, 1463 (11th Cir. 1987), and are "presumed valid." *El Mezain*, 664 F.3d at 568; *Duggan*, 743 F.2d at 77 & n.6; *Nicholson*, 2010 WL 1641167, at *5; *accord United States v. Campa*, 529 F.3d 980, 993 (11th Cir. 2008); *Warsame*, 547 F.Supp.2d at 990 ("a presumption of validity [is] accorded to the certifications"). When a FISA application is presented to the FISC, "[t]he FISA Judge, in reviewing the application, is not to second-guess the executive branch official's certification that the objective of the surveillance is foreign intelligence information." *Duggan*, 743 F.2d at 77. Likewise, Congress intended that the reviewing district court should "have no greater authority to second-guess the executive branch's certifications than has the FISA judge." *Id; see also In re Grand Jury Proceedings*, 347

---

[34] *Accord United States v. Sherifi*, 793 F. Supp. 2d 751, 760 (E.D.N.C. 2011); *Nicholson*, 2010 WL 1641167, at *5; *Warsame*, 547 F. Supp. 2d at 990; *Rosen*, 447 F.Supp.2d at 545; *Kashmiri*, 2010 WL 4705159, at *1.

F.3d at 204-05; *Badia*, 827 F.2d at 1463; *Rahman*, 861 F. Supp. at 250; *IARA*, 2009 WL 5169536, at *4; *Kashmiri*, 2010 WL 4705159, at *1.

The district court's review should determine whether the certifications were made in accordance with FISA's requirements. *See United States v. Ahmed*, No. 06-CR-00147, 2009 U.S. Dist. LEXIS 120007, at *20 ("the [c]ourt is not to second-guess whether the certifications were correct, but merely to ensure they were properly made"); *see also Campa*, 529 F.3d at 993 ("in the absence of a *prima facie* showing of a fraudulent statement by the certifying officer, procedural regularity is the only determination to be made if a non-United States person is the target"). If the target is a United States person, then the district court should also ensure that each certification is not "clearly erroneous." *Id.* at 994; *Duggan*, 743 F.2d at 77; *Kashmiri*, 2010 WL 4705159, at *2. A certification is clearly erroneous only when "the reviewing court on the [basis of the] entire evidence is left with the definite and firm conviction that a mistake has been committed." *United States v. U.S. Gypsum Co.*, 333 U.S. 364, 395 (1948); *United States v. Ruiz-Gaxiola*, 623 F.3d 684, 693 (9th Cir. 2010); *see United States v. IARA*, 2009 WL 5169536, at *4.

3. FISA's "Significant Purpose" Standard is Constitutional

The defendant challenges the constitutionality of the "significant purpose" test as an unreasonable search under the Fourth Amendment. (Docket No. 92 at 7, n.2). But the constitutionality of the "significant purpose" test has been repeatedly upheld as reasonable under the Fourth Amendment. *See Abu- Jihaad*, 630 F.3d 120 (citing cases). In fact, every court that has addressed this issue except one has held the significant-purpose test is reasonable under the Fourth Amendment. *See, e.g., Duka*, 2011 WL 6794022, at *10 ("the dispositive issue is whether the 'significant purpose' test is reasonable. . . . We agree with our sister courts of appeals and the

Foreign Intelligence Surveillance Court of Review that the amended FISA's 'significant purpose' standard is reasonable under the Fourth Amendment."); *Abu Jihaad,* 630 F.3d at 128 ("We conclude simply that FISA's 'significant purpose' requirement . . . is sufficient to ensure that the executive may only use FISA to obtain a warrant when it is in good faith pursuing foreign intelligence gathering [and the] fact that the government may also be pursuing other purposes, including gathering evidence for criminal prosecution, compels no different conclusion"); *United States v. Ning Wen*, 477 F.3d 896, 897 (7th Cir. 2007); *Damrah*, 412 F.3d at 625; *In re Sealed Case,* 310 F.3d 717, 746 (Foreign Intel. Surv. Ct. Rev. 2002); *Mubayyid,* 521 F. Supp. 2d at 139; *United States v. Marzook*, 435 F. Supp. 2d 778, 786 (N.D. Ill. 2006); *Benkahla*, 437 F. Supp. 2d at 554.[35]

As the Third Circuit noted in *Duka*, the "significant purpose" standard "reflects a balance struck by Congress . . . to promote coordination between intelligence and law enforcement officials in combating terrorism, acknowledging that, as a practical matter, these functions inevitably overlap." 2011 WL 6794022, at *10. The *Duka* Court noted that *United States v. U.S. Dist. Ct. (Keith)*, 407 U.S. 297, 322-23 (1972), required that Congress's judgment be accorded "some additional measure of deference" by the courts, adding "even leaving Congress's judgment

---

[35] The lone exception is *Mayfield v. United States,* 504 F. Supp. 2d 1023 (D. Or. 2007) – a case relied upon by defendant - which was vacated on appeal. *Mayfield v. United States*, 599 F.3d 964, 973 (9th Cir. 2010). Addressing *Mayfield*, the *Duka* Court stated: "Because the Ninth Circuit Court of Appeals vacated the judgment in that case. . . it is no longer good law and we do not address it." *United States v. Duka*, 2011 WL 6794022, at *5, n. 7.

aside, we conclude that FISA's 'significant purpose' standard is reasonable in light of the government's legitimate national security goals." *Id.*

Prior to its amendment in 2001, FISA required that the Government certify that "the purpose" of the surveillance was the acquisition of foreign intelligence information. Several courts interpreted this to require the government show acquisition of foreign intelligence was the primary purpose; drawing from the law governing warrantless searches pursuant to the Executive's Article II foreign-affairs powers prior to the enactment of FISA. *See, e.g.*, *Abu Jihaad*, 630 F.3d at 121. In that context, warrantless surveillance was conducted as an exception to the Fourth Amendment, and was therefore limited by the scope of the Constitution's grant of authority to the Executive to conduct foreign affairs. *United States v. Truong Dinh Hung*, 629 F.2d 908, 912-916 (4th Cir. 1980).[36] However, none of those cases held that the primary-purpose test was constitutionally mandated; *see Duggan*, 743 F.2d at 77; *Pelton*, 835 F.2d at 1075-76;

---

[36] In *Truong*, the Fourth Circuit was presented with wholly warrantless surveillance, carried out by the Executive Branch unilaterally and without any judicial involvement whatsoever. The Court crafted the "primary purpose" test to identify the circumstances in which the Executive Branch may constitutionally dispense with judicial oversight altogether. This case, in contrast, involves the constitutional prerequisites for surveillance conducted pursuant to the detailed statutory scheme created by FISA, with its elaborate sets of procedures and rules that subject foreign intelligence surveillance to judicial oversight and approval. There is nothing in *Truong*'s reasoning to suggest that the judicially safeguarded FISA process requires the alternative safeguard of a "primary purpose" limitation that was found to be appropriate when the judiciary was completely excluded from the process.

Badia, 827 F.2d at 1464; *Johnson*, 952 F.2d at 572;[37] and as the Second Circuit has explicitly stated, "in *Duggan*, we construed FISA's original reference to electronic surveillance for 'the purpose' of obtaining foreign intelligence information, as a 'requirement that foreign intelligence information be the *primary* objective . . . we were identifying Congress's intent in enacting FISA, not a constitutional mandate. . . . In short, nothing in *Duggan* erected a constitutional bar to Congress reconsidering and reframing the purpose requirement of FISA." *Abu Jihaad*, 630 F.3d at 123. By interpreting "the purpose" to mean "the primary purpose" – and not to mean the sole purpose – the cases recognized that a FISA could have an additional purpose other than the acquisition of foreign intelligence information, such as criminal investigation and prosecution.

Defendant urges the Court to determine "whether the collection of foreign intelligence information was either a 'significant' or the 'primary' purpose of the FISA surveillance, or whether [the] criminal investigation of a local money remitter motivated the FISA surveillance." (Docket No. 92 at 21-22) (emphasis added). However, FISA requires the Court to review the FISA materials to determine only whether a significant purpose of the collections was to obtain foreign intelligence information. *See supra* at p.12. Moreover, the fact that criminal prosecution

---

[37] In *Johnson*, the First Circuit actually construed the purpose requirement in the negative, holding that "the investigation of criminal activity cannot be the primary purpose" of FISA surveillance. *Id.*

is one of the purposes for the FISA is not fatal.[38] *See Abu Jihaad*, 630 F.3d at 128-29; *In re Sealed Case,* 310 F.3d at 735.

The *Abu-Jihaad* court rejected the argument that FISA is unconstitutional because it does not require certification of a primary purpose to obtain foreign intelligence information and stated:

> We conclude that FISA's significant purpose requirement . . . is sufficient to ensure that the executive may only use FISA to obtain a warrant when it is in good faith pursuing foreign intelligence gathering. . . *The fact that the government may also be pursuing other purposes, including gathering evidence for criminal prosecution, compels no different conclusion.* We reject the argument that FISA is unconstitutional because is does not require certification of a primary purpose to obtain foreign intelligence information.

Id. at 128-29 (emphasis added).

Here the FISA certifications and the balance of the materials before the Court amply demonstrate that a significant purpose was to obtain foreign intelligence information.[39]

4. Probable Cause

Defendant concedes that FISA's probable cause standard is not the same as it is for evidence of a crime; Docket No. 92 at 9, 14-15; he nevertheless directs the Court to *Maryland v. Pringle*, 540 U.S. 366, 371 (2003), a case addressing the standard for criminal probable cause. *Pringle* however, is inapplicable. FISA requires a finding of probable cause that the target is a foreign power or an agent of a foreign power and that each facility or property at which the

---

[38] A criminal prosecution motive is only fatal if the Court finds the government's certification that the significant purpose certification in the FISA application is clearly erroneous. *See Abu-Jihaad,* 630 F.3d at 128.

electronic surveillance and/or physical search is directed is being used, owned, and/or possessed, or is about to be used, owned, and/or possessed, by a foreign power or an agent of a foreign power. *See supra* at 15. It is this standard, not the criminal standard addressed in *Pringle*, that applies to this Court's review of the FISC's probable cause determination. *See United States v. Cavanagh*, 807 F.2d. 787, 790 (9th Cir. 1987) (citing *Keith*, 407 U.S. at 322); *El-Mezain*, 664 F.3d, at 564; *Abu-Jihaad*, 630 F.3d at 130-31; *Duka*, 2011 WL 6794022, at *5. This "different, and arguably lower, probable cause standard . . . reflects the purpose for which FISA search orders are issued." *Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *22.

[CLASSIFIED MATERIAL REDACTED]

a. The Fourth Amendment

FISA's probable cause standard also satisfies the reasonableness requirement of the Fourth Amendment even though it does not depend upon evidence of a crime. In *Keith*, 407 U.S. 322-23, the Supreme Court recognized that "[d]ifferent standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens." *Keith*, 407 U.S. at 322-23 (recognizing that domestic security surveillance "may involve different policy and practical considerations than the surveillance of 'ordinary crime'"). In *Keith*, the Supreme Court acknowledged that: (1) the "focus of . . . surveillance [in domestic security investigations] may be less precise than that directed against more conventional types of crime"; (2) unlike ordinary

---

[39] **[CLASSIFIED MATERIAL REDACTED]**

criminal investigations, "the gathering of security intelligence is often long range and involves the interrelation of various sources and types of information;" and (3) the "exact targets of such surveillance may be more difficult to identify" than in surveillance operations of ordinary crimes under Title III. *Id.* FISA was enacted partly in response to *Keith.* In constructing FISA's framework, Congress addressed *Keith's* question whether departures from traditional Fourth Amendment procedures "are reasonable, both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens," and "concluded that such departures are reasonable." *See* S. Rep. No. 95-701, 95th Cong., 2d Sess., at 11, (quoting *Keith* at 323) *reprinted in* 1978 U.S.C.C.A.N. 3973, 3980 (1978) ("Senate Report").

Courts have universally agreed – relying on *Keith* -- that FISA's unique probable cause standard comports with the Fourth Amendment. *See, e.g.*, *Ning Wen,* 477 F.3d at 898 (holding that FISA is constitutional despite is definition of probable cause that does not depend upon whether a domestic crime has been committed); *Damrah,* 412 F.3d at 624 (rejecting claim that FISA procedures violate the Fourth Amendment); *Isa*, 923 F.2d at 1302 (affirming district court's conclusion that FISA collection did not violate the Fourth Amendment and rejecting defendant's challenge to FISA's lower probable cause threshold); *Pelton*, 835 F.2d at 1075 (FISA's procedures compatible with the Fourth Amendment "despite allowing surveillance on less than traditional probable cause"); *Duggan*, 743 F.2d at 73-74 (holding that FISA's less stringent probable cause standard does not violate the Fourth Amendment); *Mubayyid*, 521 F. Supp. 2d at 135-41 (rejecting claim that FISA violates the Fourth Amendment's judicial review, probable cause, notice, and particularity requirements); *Falvey*, 540 F. Supp. at 1311-14 (finding that FISA procedures satisfy the Fourth Amendment's warrant requirement). *See also In re Sealed Case*,

310 F.3d at 738, 746 (finding that while many of FISA's requirements differ from those in Title III, few of those differences have constitutional relevance).

b. FISA Materials Are Subject to the "Good-Faith" Exception

Even if this Court determines that a particular FISC order was not supported by probable cause, or that one or more of the FISA certification requirements were not in fact met, the Government respectfully submits that the FISA materials – and the evidence obtained or derived from the FISA collection – are, nonetheless, admissible under the "good faith" exception to the exclusionary rule articulated in *United States v. Leon*, 468 U.S. 897 (1984).[40] The Seventh Circuit, relying on *Leon*, held that federal officers were entitled to rely in good faith on a FISA warrant. *Ning Wen*, 477 F.3d at 897. As the court noted:

> [T]he exclusionary rule must not be applied to evidence seized on the authority of a warrant, even if the warrant turns out to be defective, unless the affidavit supporting the warrant was false or misleading, or probable cause was so transparently missing that "no reasonably well trained officer [would] rely on the warrant."

Id. (quoting *Leon)* (alteration in original); *see also Duka*, 2011 WL 6794022, at *12 (citing *Leon* and stating that even if FISA were unconstitutional, evidence derived therefrom would be admissible under the exclusionary rule); *Duggan*, 743 F.2d at 77 n.6 (opining that *Franks*

---

[40] "[E]ven if we were to conclude that amended FISA is unconstitutional, evidence derived from it would nevertheless be admissible in the government's case. . . . The exclusionary rule precludes the admission of evidence tainted by a Fourth Amendment violation" only in those cases where its application will deter police misconduct. *Duka*, 2011 WL 6794022, at *12, citing *Leon*, 468 U.S. at 918.

principles apply to review of FISA orders); *Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *25 n.8 ("[t]he FISA evidence obtained . . . would be admissible under *Leon's* 'good faith' exception to the exclusionary rule were it not otherwise admissible under a valid warrant").

[CLASSIFIED MATERIAL REDACTED]

c. The Court Should Summarily Reject the Residual Constitutional Challenge

Defendant asserts a residual challenge to the FISA broadly claiming "the government may have violated . . . the First and/or the Fourth Amendments in manners unknown. . . ." The Court should summarily reject defendant's conclusory assertions that FISA may be unconstitutional. In *In re Grand Jury Proceedings*, 347 F.3d at 206, the defendant alleged FISA was unconstitutional in conclusory fashion and without citation to authority. The Court refused to consider the constitutional challenges stating the appellant was only "pointing a finger at a particular clause." *Id.*

Additionally, we note that we are unaware of any successful Constitutional challenge to FISA. In *Ahmed,* 2009 U.S. Dist. LEXIS 120007 at *30, the Court rejected a motion for disclosure of FISA materials and suppression succinctly stating: "[t]he Defendants do not cite to any authority for [the proposition that FISA is unconstitutional] because there is none. Every court that has considered FISA's constitutionality has upheld the statute from challenges under the Fourth, Fifth, and Sixth Amendments."

Moreover, as previously demonstrated, there is no decision that upholds a challenge to FISA on Fourth Amendment grounds. *See supra,* Section III.B.3 & 4. If FISA is valid under the Fourth Amendment, then there can be no independent claim that it violates the First Amendment rights of the FISA targets. *See ACLU Foundation,* 952 F.2d at 471. *See also United States v. Mayer*, 503 F.3d 740, 750 (9th Cir. 2007)(when undercover activity is lawful under the Fourth Amendment ,*a fortiori* it does not violate the First Amendment).

For these reasons, the Court should reject Moalin's residual constitutional challenge.

IV. THE FISA COLLECTION WAS BOTH LAWFULLY AUTHORIZED AND LAWFULLY CONDUCTED

[CLASSIFIED MATERIAL REDACTED][41]

A. THE CERTIFICATIONS

Each FISA application was supported by a certification signed by a duly-authorized, high-ranking official of the United States Government. The FISC properly determined that each of those certifications complied with FISA's requirements that: (1) the certifying official deemed the information sought to be foreign intelligence information; (2) a significant purpose of the surveillance or search was to obtain foreign intelligence information; and (3) the information sought could not reasonably have been obtained by normal investigative techniques. *See* 50 U.S.C. §§ 1804(a)(6)(A)-(C), 1823(a)(6)(A)-(C). As noted above, certifications submitted in support of a FISA application should be "presumed valid," and neither the FISC nor a reviewing

---

[41] **[CLASSIFIED MATERIAL REDACTED]**

district court should "second-guess the executive branch official's certification that the objective of the surveillance is foreign intelligence information." *Duggan*, 743 F.2d at 77 & n. 6; *Gowadia*, 2009 WL 1649714, at *2-3. In reviewing the certifications, a district court should apply the same standard as the FISC, which, because the targets are U.S. persons, is the "clearly erroneous" standard. *Badia*, 827 F.2d at 1463; *see* 50 U.S.C. §§ 1805(a)(1)-(4), 1824(a)(1)-(4). As discussed below, there is ample information, both in the certifications themselves and in the declarations, to demonstrate that the certifications were not clearly erroneous.

1. Foreign Intelligence Information

[CLASSIFIED MATERIAL REDACTED][42] [43]

2. "A Significant Purpose"

[CLASSIFIED MATERIAL REDACTED][44] [45] [46] [47]

3. Information Not Reasonably Obtainable Through Normal Investigative Techniques

[CLASSIFIED MATERIAL REDACTED][48]

---

[42] **[CLASSIFIED MATERIAL REDACTED]**

[43] **[CLASSIFIED MATERIAL REDACTED]**

[44] **[CLASSIFIED MATERIAL REDACTED]**

[45] **[CLASSIFIED MATERIAL REDACTED]**

[46] **[CLASSIFIED MATERIAL REDACTED]**

[47] **[CLASSIFIED MATERIAL REDACTED]**

For the above reasons, the FISC properly found that the certifications were not clearly erroneous.

B. THE FISA APPLICATIONS ESTABLISHED PROBABLE CAUSE

[CLASSIFIED MATERIAL REDACTED][49]

1. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

a. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

2. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

a. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED][50] [51] [52] [53] [54] [55]

---

[48] **[CLASSIFIED MATERIAL REDACTED]**

[49] **[CLASSIFIED MATERIAL REDACTED]**

[50] **[CLASSIFIED MATERIAL REDACTED]**

[51] **[CLASSIFIED MATERIAL REDACTED]**

[52] **[CLASSIFIED MATERIAL REDACTED]**

[53] **[CLASSIFIED MATERIAL REDACTED]**

[54] **[CLASSIFIED MATERIAL REDACTED]**

b. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

i. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED][56] [57]

ii. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

iii. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED][58]

iv. [CLASSIFIED MATERIAL REDACTED]

---

[55] **[CLASSIFIED MATERIAL REDACTED]**

[56] **[CLASSIFIED MATERIAL REDACTED]**

[57] **[CLASSIFIED MATERIAL REDACTED]**

[58] **[CLASSIFIED MATERIAL REDACTED]**

[CLASSIFIED MATERIAL REDACTED][59] [60]

v. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED][61] [62] [63]

c. Defendant's Legal Arguments Are Baseless

i. Defendant's Position Regarding the Reliability of Intelligence is Baseless

The defendant identifies what he terms "factors and principles" that should guide the Court's review of the FISC's probable cause determinations. (*See* Docket No. 92 at 15.) Initially, he argues that raw intelligence is generally unreliable because: (1) it is often not attributed to any specific source; (2) it may be based on hearsay and speculation; and (3) the motivation behind such reporting is not transparent.

[CLASSIFIED MATERIAL REDACTED][64]

---

[59] **[CLASSIFIED MATERIAL REDACTED]**

[60] **[CLASSIFIED MATERIAL REDACTED]**

[61] **[CLASSIFIED MATERIAL REDACTED]**

[62] **[CLASSIFIED MATERIAL REDACTED]**

[63] **[CLASSIFIED MATERIAL REDACTED]**

[64] **[CLASSIFIED MATERIAL REDACTED]**

ii. Defendant's Position Regarding "Illegitimate" or Unconstitutional Means of Electronic Surveillance Moot

[CLASSIFIED MATERIAL REDACTED]

iii. [CLASSIFIED MATERIAL REDACTED]

Moalin claims he was targeted for FISC-authorized surveillance in violation of FISA's stipulation that no United States person may be considered a foreign power or an agent of a foreign power solely on the basis of activities protected by the First Amendment. Docket No 92 at 18-19 (*citing* 50 U.S.C. §§ 1805(a)(2)(A), 1824(a)(2)(A)). Although *protected* First Amendment activities cannot form the *sole* basis for FISC-authorized electronic surveillance or physical search, not all speech-related activities fall within the protection of the First Amendment. *See infra* at 70. Moreover, even activities that fall within the First Amendment's protection may be considered by the FISC if, as was the case here, the application sets forth other activity indicating that the proposed target is an agent of a foreign power. *United States v. Dumesi*, 424 F.3d 566, 579 (7th Cir. 2005); *Rosen*, 447 F. Supp. 2d at 549-50; *Rahman*, 861 F. Supp. at 252, *aff'd*, 189 F.3d 88 (2d Cir. 1999).

[CLASSIFIED MATERIAL REDACTED]

In any event, rather than supporting Moalin's position, the FIG Assessment outlines activity plainly not protected by the First Amendment, including fundraising for a designated FTO:

> The San Diego FIG assess that *Moalin, . . . is the most significant al-Shabaab fundraiser in the San Diego Area of Operations*. . . .The San Diego FIG assesses, that Moalin likely supported now deceased senior al-Shabaab leader Aden Ayrow due to Ayrow's tribal affiliation . . .rather than his position with al-Shabaab. The San Diego FIG assesses, based on reporting that *Moalin has provided direction*

regarding financial accounts to be used when transferring funds overseas that he also serves as a controller for the US-based al-Shabaab fundraising network.

(emphasis added). It is well-established that fundraising is conduct and not protected speech. *See, e.g.*, *United States v. Afshari*, 426 F.3d 1150, 1161 (9th Cir. 2005); *United States v. Chandia*, 514 F.3d 365, 371 (4th Cir. 2007); *Hammoud*, 381 F.3d at 330.

[CLASSIFIED MATERIAL REDACTED]

4. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

5. [CLASSIFIED MATERIAL REDACTED]
[CLASSIFIED MATERIAL REDACTED][65]

a. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED][66] [67] [68]

---

[65] **[CLASSIFIED MATERIAL REDACTED]**

[66] **[CLASSIFIED MATERIAL REDACTED]**

[67] **[CLASSIFIED MATERIAL REDACTED]**

[68] "Emergency employment" is a term that appears in the statute. *See* 50 U.S.C. §§ 1805(f), 1824(e) (effective March 9, 2006, to July 9, 2008).

b. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED][69]

c. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED][70] [71] [72]

6. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

7. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

a. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED][73] [74] [75]

---

[69] **[CLASSIFIED MATERIAL REDACTED]**

[70] **[CLASSIFIED MATERIAL REDACTED]**

[71] **[CLASSIFIED MATERIAL REDACTED]**

[72] **[CLASSIFIED MATERIAL REDACTED]**

[73] **[CLASSIFIED MATERIAL REDACTED]**

[74] **[CLASSIFIED MATERIAL REDACTED]**

[75] **[CLASSIFIED MATERIAL REDACTED]**

b. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

i. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED][76] [77]

ii. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

iii. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED][78] [79] [80]

iv. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED][81] [82]

c. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

8. [CLASSIFIED MATERIAL REDACTED]

---

[76] **[CLASSIFIED MATERIAL REDACTED]**

[77] **[CLASSIFIED MATERIAL REDACTED]**

[78] **[CLASSIFIED MATERIAL REDACTED]**

[79] **[CLASSIFIED MATERIAL REDACTED]**

[80] **[CLASSIFIED MATERIAL REDACTED]**

[81] **[CLASSIFIED MATERIAL REDACTED]**

[82] **[CLASSIFIED MATERIAL REDACTED]**

[CLASSIFIED MATERIAL REDACTED][83]

a. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED][84] [85] [86]

9. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

C. THE FISA COLLECTION WAS LAWFULLY CONDUCTED

This Court's *in camera*, *ex parte* review of the FISA materials will demonstrate not only that the FISA collection was lawfully authorized, but also that it was lawfully conducted. That is, the FISA-obtained or -derived information that will be offered into evidence in this case was acquired, retained, and disseminated by the FBI in accordance with FISA's minimization requirements, and the implementing standard minimization procedures ("SMPs") promulgated by the Attorney General and approved by the FISC.

1. Minimization

[CLASSIFIED MATERIAL REDACTED][87]

---

[83] **[CLASSIFIED MATERIAL REDACTED]**

[84] **[CLASSIFIED MATERIAL REDACTED]**

[85] **[CLASSIFIED MATERIAL REDACTED]**

[86] **[CLASSIFIED MATERIAL REDACTED]**

[87] **[CLASSIFIED MATERIAL REDACTED]**

Under FISA and both sets of SMPs, minimization "may occur at any of several stages, including recording, logging, indexing, or dissemination." *IARA*, 2009 WL 5169536, at *6 (citing *Kevork*, 634 F. Supp. at 1017); Senate Report at 40; current SMPs,, Section I.A., pp. 1-2. At the acquisition stage, FISA does not "prohibit the use of automatic tape recording equipment." *Rahman*, 861 F. Supp. at 252; *Kevork*, 634 F. Supp. at 1017. Indeed, the FISC has noted that FISA surveillance devices are normally left on continuously and that consequently minimization occurs (under the old SMPs) during the logging and indexing of the pertinent communications.[88] *See In re Sealed Case*, 310 F.3d at 740.

Generally, after a communication is collected and reduced to an intelligible form (*e.g.*, by transcription or translation), it is reviewed to determine whether it contains, or might contain, foreign intelligence information. *See In re All Matters Submitted to FISC*, 218 F. Supp. 2d 611, 618 (Foreign Intel. Surv. Ct. Rev. 2002); *rev'd on other grounds by In re Sealed Case*, 310 F.3d at 717. If it contains such foreign intelligence information, or is necessary to understand or assess foreign intelligence information, the communication is not subject to minimization; *i.e.*, it "meets the standard" for retention. Moreover, FISA expressly states that the Government is not required to minimize information that is "evidence of a crime," whether or not it is also foreign intelligence information. 50 U.S.C. § 1801(h)(3); *see also Isa*, 923 F.2d at 1305.

---

[88] **[CLASSIFIED MATERIAL REDACTED]**

[CLASSIFIED MATERIAL REDACTED][89] [90] [91] [92] [93]

The degree to which information is required to be minimized varies somewhat given the specifics of a particular investigation, such that less minimization at the acquisition and retention stages is justified when "the investigation is focusing on what is thought to be a widespread conspiracy" and more extensive surveillance is necessary "to determine the precise scope of the enterprise." *In re Sealed Case*, 310 F.3d at 741; *Bin Laden*, 126 F. Supp. 2d at 286 ("[m]ore extensive monitoring and 'greater leeway' in minimization efforts are permitted in a case [involving] . . . [a] 'world-wide, covert and diffuse . . . international terrorist group.'"). Furthermore, the activities of foreign powers and their agents are often not obvious from an initial or cursory overhear of conversations. To the contrary, agents of foreign powers frequently engage in coded communications, compartmentalized operations, the use of false identities and other practices designed to conceal the breadth and aim of their operations, their organization, activities and plans. *See, e.g.*, *United States v. Salameh*, 152 F.3d 88, 154 (2d Cir. 1998) (noting that two

---

[89] **[CLASSIFIED MATERIAL REDACTED]**

[90] **[CLASSIFIED MATERIAL REDACTED]**

[91] **[CLASSIFIED MATERIAL REDACTED]**

[92] (U) *See* H.R. Rep. No. 95-1283, 95th Cong., 2d Sess., Pt. 1 ("House Report") (1978) at 58 (noting that minimization can occur by rendering the information "not retrievable by the name of the innocent person."). The House Report is not reprinted in U.S. Code Congressional & Administrative News; however, we have provided the pages of the report cited in this memorandum at Attachment A.

[93] **[CLASSIFIED MATERIAL REDACTED]**

conspirators involved in the 1993 bombing of the World Trade Center in New York referred to the bomb plot as the "study" and to terrorist materials as "university papers"). As one court explained, "[i]nnocuous-sounding conversations may in fact be signals of important activity [and] information on its face innocent when analyzed or considered with other information may become critical." *Kevork*, 634 F. Supp. at 1017 (quoting House Report at 55); *see also In re Sealed Case*, 310 F.3d at 740-41; *Bin Laden*, 126 F. Supp. 2d at 286. Likewise, "individual items of information, not apparently significant when taken in isolation, may become highly significant when considered together over time." *Kevork*, 634 F. Supp. at 1017; *Rahman*, 861 F. Supp. at 252-53 (rejecting the notion that the "wheat" could be separated from the "chaff" while the "stalks were still growing"). This is especially true where the individuals involved use codes or cryptic language. *See, e.g.*, *Hammoud*, 381 F.3d at 334 ("[a] conversation that seems innocuous on one day may later turn out to be of great significance, particularly if the individuals involved are talking in code"); *Bin Laden*, 126 F. Supp. 25 at 286; *Kevork*, 634 F. Supp. at 1017; *Thomson*, 752 F. Supp. at 81 (permissible to retain and disseminate "bits and pieces" of information until their "full significance becomes apparent"). As a result, "courts have construed 'foreign intelligence information' broadly and sensibly allowed the government latitude in its determination of what is foreign intelligence information." *Rosen*, 447 F. Supp. 2d at 551; *IARA*, 2009 WL 5169536, at *4.

Moreover, as noted above, FISA expressly states that the Government is not required to minimize information that is "evidence of a crime." 50 U.S.C. §§ 1801(h)(3), 1821(4)(c). As a result, to the extent that certain communications of a United States person may be evidence of a

crime or may otherwise establish an element of a substantive or conspiratorial offense, such communication need not be minimized. *Isa*, 923 F.2d at 1305.

The nature of the foreign intelligence information sought also impacts the amount of information regarding a United States person that can properly be retained and disseminated. As Congress explained, there is a legitimate need to conduct a thorough post-acquisition review of FISA information that involves a United States person who is acting as an agent of a foreign power:

> It is "necessary" to identify anyone working with him in this network, feeding him information, or to whom he reports. Therefore, it is necessary to acquire, retain and disseminate information concerning all his contacts and acquaintances and his movements. Among his contacts and acquaintances, however, there are likely to be a large number of innocent persons. Yet, information concerning these person must be retained at least until it is determined that they are not involved in the clandestine intelligence activities and may have to be disseminated in order to determine their innocence.

House Report at 58. Indeed, courts have cautioned that, when a United States person communicates with an agent of a foreign power, the Government would be "remiss in meeting its foreign counterintelligence responsibilities" if it did not thoroughly "investigate such contacts and gather information to determine the nature of those activities." *Thomson*, 752 F. Supp. at 82.

Congress also recognized that agents of a foreign power are often very sophisticated and skilled at hiding their activities. *See Thomson*, 752 F. Supp. at 81 (quoting House Report at 58). Accordingly, to pursue leads, Congress intended that the Government be given "a significant degree of latitude" with respect to the "retention of information and the dissemination of information between and among counterintelligence components of the Government." *Id.*

In light of these realities, Congress recognized that minimization efforts by the Government can never be free of mistake, because "no electronic surveillance can be so conducted that innocent conversations can be totally eliminated." Senate Report at 39. The Fourth Circuit reached the same conclusion in *Hammoud*, 381 F.3d at 334, stating that the "mere fact that innocent conversations were recorded, without more, does not establish that the government failed to appropriately minimize surveillance."[94]

Accordingly, in reviewing the adequacy of minimization efforts, the test to be applied is neither whether innocent conversations were intercepted, nor whether mistakes were made with respect to particular communications. Rather, as the United States Supreme Court stated in the context of Title III surveillance, there should be an "objective assessment of the [agents'] actions in light of the facts and circumstances confronting [them] at the time." *Scott v. United States*, 436 U.S. 128, 136 (1978). In the context of FISA minimization one Court of Appeals has determined that the test of compliance is whether a good faith effort to minimize was made. *Hammoud*, 381 F.3d at 334 ("[t]he minimization requirement obligates the Government to make a good faith effort to minimize the acquisition and retention of irrelevant information"); *see also* Senate Report at 39-40 (stating that the court's role is to determine whether "on the whole, the agents

---

[94] The reason is that although "the minimization requirement obligates the Government to make a good faith effort to minimize . . . it is not always immediately clear into which category a particular conversation falls. A conversation that seems innocuous on one day may later turn out to be of great significance, particularly, if the individuals involved are talking in code." *Hammoud*, 381 F.3d at 334 (citing Senate Report at 39-40).

have shown a high regard for the right of privacy and have done all they reasonably could do to avoid unnecessary intrusion"); *IARA*, 2009 WL 5169536, at *6 (quoting Senate Report at 39-40).

Moreover, absent evidence that there has been a complete disregard for the minimization procedures, suppression is not the appropriate remedy with respect to those communications that were properly acquired, retained, or disseminated. Indeed, Congress intended that any suppression remedy should apply only to the "evidence which was obtained unlawfully." House Report at 93. FISA's legislative history reflects that Congress intended only this limited sanction for errors of minimization:

> As the language of the bill makes clear, only that evidence which was obtained unlawfully or derived from information obtained unlawfully would be suppressed. If, for example, some information should have been minimized but was not, only that information should be suppressed; the other information obtained lawfully should not be suppressed.

Id; *accord IARA*, 2009 WL 5169536, at *7 ("this Court declines to suppress evidence obtained through FISA warrants properly issued and conducted"); *see also United States v. Falcone*, 364 F. Supp. 877, 886-87 (D.N.J. 1973), *aff'd*, 500 F.2d 1401 (3d Cir. 1974) (Title III).

2. The FISA Collection was Appropriately Minimized

[CLASSIFIED MATERIAL REDACTED]

V. CONCLUSION

The Attorney General's declaration in this case establishes that disclosure or an adversary hearing would harm the national security of the United States. Therefore, FISA mandates that this Court conduct an *in camera*, *ex parte* review of the challenged FISA materials to determine whether the collection was both lawfully authorized and conducted. In conducting that review,

the Court may disclose the FISA materials "only where such disclosure is necessary to make an accurate determination of the legality of the surveillance [or search]." *See* 50 U.S.C. §§ 1806(f), 1825(g). To date, no Court has ever ordered the disclosure of FISA materials and there is nothing extraordinary about this case that would warrant it be the first to disclose such materials. *See* 50 U.S.C. §§ 1806(f), 1825(g); *El-Mezain*, 664 F.3d, at 566; *Abu-Jihaad*, 630 F.3d at 129; *Belfield*, 692 F.2d at 147; *Kashmiri*, 2010 WL 4705159 at *2; *Nicholson*, 2010 WL 1641167, at *4; *IARA*, 2009 WL 5169536 at *3-4.

Courts have uniformly upheld FISA against Constitutional challenge finding: 1) that FISA's provisions for *in camera, ex parte* review comport with due process; *see, e.g.*, *El-Mezain*, 664 F.3d, at 566-67; *Abu Jihaad*, 630 F.3d at 129 (no violation of due process in district court's *in camera, ex parte* determination of FISA suppression motion); *Damrah*, 412 F.3d, at 624; 2) that FISA's probable cause standard and significant purpose provisions satisfy the requirements of the Fourth Amendment. *See supra* at pp. 40-47.

The Court's *in camera, ex parte* review will demonstrate that the Moalin and Yusuf FISA's were lawfully authorized and lawfully conducted. Indeed, we are unaware of any case in which a Court has ordered suppression of FISA-derived materials. Even if this Court were to determine that any part of the FISA collection had not been lawfully authorized or lawfully conducted, the FISA evidence would nevertheless be admissible under the "good faith" exception to the exclusionary rule articulated in *Leon*, 468 U.S. 897 (1984). *See Ning Wen*, 477 F.3d at 897 (holding that the *Leon* good-faith exception applies to FISA orders); *Mubayyid*, 521 F. Supp. 2d at 140 n. 12 (noting that the Government could proceed in good-faith reliance on FISA orders even

if FISA were deemed unconstitutional); *Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *25 n. 8; *Nicholson*, 2010 WL 1641167, at *6.

Based on the foregoing analysis, the Government respectfully submits that the Court should: (1) conduct an *in camera*, *ex parte* review of the FISA dockets and the Government's classified submission; (2) find that the FISA surveillance was lawfully authorized and lawfully conducted in compliance; (3) hold that disclosure of the FISA dockets and the Government's classified submissions to the defense is not required because the Court is able to make an accurate

determination of the legality of the surveillance without disclosing the FISA dockets or any portions thereof; (4) order that the FISA dockets and the Government's classified submissions be maintained under seal by the Court Security Officer or his/her designee; and (5) deny the defendant's motion.[95]

Dated: February 17, 2012

Respectfully submitted,

LAURA E. DUFFY
United States Attorney

By: /s/ William P. Cole
WILLIAM P. COLE
CAROLINE P. HAN
Assistant United States Attorneys

/s/ Steven P. Ward
STEVEN P. WARD
Trial Attorney
Counterterrorism Section
National Security Division

Attorneys for Plaintiff
United States of America

---

[95] A district court order requiring the disclosure of FISA materials is a final order for purposes of appeal. *See* 50 U.S.C. § 1806(h). Should the Court conclude that disclosure of any item within any of the FISA materials may be required, given the significant national security consequences that would result from such disclosure, the Government would expect to pursue an appeal. Accordingly, the Government respectfully requests that the Court indicate its intent to do so before issuing any order, that any such order be issued in such a manner that the United States has sufficient notice to file an appeal prior to any actual disclosure, and that any such order be stayed pending an appeal.