UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA - v. – SAJMIR ALIMEHMETI, a/k/a "Abdul Qawii," Defendant.	16 Cr. 398 (PAE)

GOVERNMENT'S UNCLASSIFIED MEMORANDUM IN OPPOSITION TO DEFENDANT'S PRETRIAL MOTION TO SUPPRESS AND FOR A *FRANKS* HEARING AND DISCLOSURE OF FISA ORDERS, APPLICATIONS, AND RELATED MATERIALS; AND MOTION FOR NOTICE OF AND DISCOVERY ABOUT THE USE OF EXECUTIVE ORDER 12333 SURVEILLANCE

JOON H. KIM
Acting United States Attorney for the
Southern District of New York
Attorney for the United States of America

Emil J. Bove III
George D. Turner
Assistant United States Attorneys

Joseph Attias
Trial Attorney, National Security Division

Chad M. Davis
Attorney Advisor, National Security Division

TABLE OF CONTENTS

TABLE OF AUTHORITIES

FEDERAL CASES

U.S. CONSTITUTION

FEDERAL STATUTES

OTHER AUTHORITIES

I. INTRODUCTION[1]

The Government is filing this unclassified Memorandum in Opposition to the Defendant's Pretrial Motion to Suppress and for a *Franks* Hearing and Disclosure of [Foreign Intelligence Surveillance Act (FISA)] Orders, Applications, and Related Materials (hereinafter Doc. 60); and Motion for Notice of and Discovery about the Use of Executive Order (E.O.) 12333 Surveillance (hereinafter Doc. 61) (together, defendant's motions). The defendant seeks: (1) suppression of the evidence derived from FISA electronic surveillance and physical search (*i.e.*, the FISA information); (2) in the alternative, a *Franks* hearing relating to the suppression motion that would entail disclosure to the defense of the FISA applications, orders, and related materials (*i.e.*, the FISA materials); and (3) notice and discovery of any E.O. 12333 information used in the instant criminal proceedings. (Docs. 60 and 61 at 1).[2]

The defendant has triggered this Court's review of the FISA materials related to the FISC-authorized electronic surveillance and physical search to determine whether the FISA information was lawfully acquired and whether the electronic surveillance and physical search were made in conformity with an order of authorization or approval.[3] Whenever "a motion is made "to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from

---

[1] (U) In light of the complexity of the issues raised by the instant motions, the Government respectfully requests permission to exceed the page limit set in the court's rules.

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

[3] The provisions of FISA that address electronic surveillance generally are found at 50 U.S.C. §§ 1801-1812; those that address physical search are found at 50 U.S.C. §§ 1821-1829. These two sets of provisions are in many respects parallel and almost identical. Citations herein are generally to the two sets of provisions in parallel, with the first citation being to the relevant electronic surveillance provision, and the second citation being to the relevant physical search provision.

electronic surveillance under FISA, the United States district court . . . shall . . . if the Attorney General files an affidavit 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). The Government is filing herewith such an affidavit in which the Attorney General claims under oath that disclosure or an adversary hearing would harm the national security of the United States, which is the prerequisite for the Court to review the FISA materials *in camera* and *ex parte*;[4] consequently, the Government respectfully submits that, for the reasons set forth hereinafter, this Court should conduct an *in camera, ex parte* review of the documents relevant to the defendant's motions in accordance with the provisions of 50 U.S.C. §§ 1806(f) and 1825(g).[5]

The Government respectfully submits that, for the reasons set forth below, and as the Court's *in camera, ex parte* review will show: (1) the electronic surveillance and physical search at issue were both lawfully authorized and lawfully conducted in compliance with FISA; (2) disclosure to the defendant of the FISA materials and the Government's classified submissions is not authorized because the Court is able to make an accurate determination of the legality of the electronic surveillance and physical search without disclosing the FISA materials or portions thereof; (3) the FISA information should not be suppressed; (4) the FISA materials should not be disclosed; and (5) no hearing is required.

---

[4] The Attorney General's affidavit ("Declaration and Claim of Privilege") is filed both publicly and as an exhibit in the Sealed Appendix to the classified filing.

[5] **[CLASSIFIED MATERIAL REDACTED]**.

A. BACKGROUND

On June 7, 2016, Sajmir Alimehmeti (Alimehmeti), also known as Abdul Qawii, was charged by indictment in the Southern District of New York with one count each of: (1) providing and attempting to provide material support to a foreign terrorist organization, in violation of 18 U.S.C. §§ 2339B and 2; and (2) passport fraud, in violation of 18 U.S.C. § 1542. (*See* Doc. 8).

[CLASSIFIED MATERIAL REDACTED].

On July 21, 2016, pursuant to 50 U.S.C. §§ 1806(c) and 1825(d), the United States provided notice to Alimehmeti and this Court that it "intends to offer into evidence, or otherwise use or disclose . . . information obtained and derived from electronic surveillance and physical search conducted pursuant to [FISA]." (*See* Doc. 14). On May 15, 2017, Alimehmeti filed his motions. (*See* Docs. 60 and 61).

[CLASSIFIED MATERIAL REDACTED].

In subsequent sections of this Memorandum, the Government will: (1) present an overview of the FISA authorities at issue in this case; (2) discuss the FISA process; (3) address the manner in which the Court should conduct its *in camera, ex parte* review of the FISA materials; (4) summarize the facts supporting the FISC's probable cause determinations with respect to the target of the electronic surveillance and physical search and to the facility(ies) targeted (all of which information is contained fully in the exhibits in the Sealed Appendix); (5) discuss the relevant minimization procedures; and (6) address the defendant's arguments in support of his motions. All of the Government's pleadings and supporting FISA materials are being submitted not only to oppose the defendant's motions, but also to support the United States' request, pursuant to FISA, that this Court: (1) conduct an *in camera, ex parte* review of

the FISA materials; (2) find that the FISA information at issue was lawfully acquired and that the electronic surveillance and physical search were conducted in conformity with an order of authorization or approval; (3) deny the defendant's request that the FISA information be suppressed; (4) order that none of the FISA materials be disclosed to the defense, and instead, that they be maintained by the United States under seal; and (5) find that the Government has fulfilled its notice and disclosure obligations.

B. OVERVIEW OF THE FISA AUTHORITIES

[CLASSIFIED MATERIAL REDACTED].

1. [CLASSIFIED MATERIAL REDACTED].

[CLASSIFIED MATERIAL REDACTED].

2. The FISC's Findings

[CLASSIFIED MATERIAL REDACTED].

II. THE FISA PROCESS

A. OVERVIEW OF FISA[6]

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 search 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 ("FISA Ct. Rev."), which is composed of three United States District or Circuit Court Judges who are designated by the Chief Justice. 50 U.S.C. § 1803(b).

[6] This Memorandum references the statutory language in effect at the time relevant to this matter.

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").[7] One change to FISA accomplished by the USA PATRIOT Act is that a high-ranking official is now required to certify that the acquisition of foreign intelligence information is "a significant purpose" of the requested surveillance. 50 U.S.C. § 1804(a)(6)(B).

FISA provides that the Attorney General may authorize the emergency employment of electronic surveillance and physical search if the Attorney General:

> (A) reasonably determines that an emergency situation exists with respect to the employment of electronic surveillance [or physical search] to obtain foreign intelligence information before an order authorizing such surveillance [or physical search] can with due diligence be obtained;
>
> (B) reasonably determines that the factual basis for the issuance of an order under this title to approve such electronic surveillance [or physical search] exists;
>
> (C) informs, either personally or through a designee, a judge having jurisdiction under [50 U.S.C. § 1803] at the time of such authorization that the decision has been made to employ emergency electronic surveillance [or physical search]; and
>
> (D) makes an application in accordance with this title to a judge having jurisdiction under section 103 as soon as practicable, but not later than seven days after the Attorney General authorizes such electronic surveillance [or physical search].

[7] Pub. L. No. 107-56, 115 Stat. 272 (2001).

50 U.S.C. §§ 1805(e)(1), 1824(e)(1).[8] Emergency electronic surveillance or physical search must comport with FISA's minimization requirements, which are discussed below. 50 U.S.C. §§ 1805(e)(2), 1824(e)(2).[9]

B. THE FISA APPLICATION

FISA provides a statutory procedure whereby the Executive Branch may obtain a judicial order authorizing the use of electronic surveillance and/or physical search within the United States where a significant purpose is the collection of foreign intelligence information.[10] 50 U.S.C. §§ 1804(a)(6)(B), 1823(a)(6)(B). Under FISA, foreign intelligence information is defined as:

> (1) information that relates to, and if concerning a United States person[11] is necessary to, the ability of the United States to protect against—
>
> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

---

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

[9] If no FISC order authorizing the electronic surveillance or physical search is issued, emergency surveillance or search must terminate when the information sought is obtained, when the FISC denies an application for an order, or after the expiration of seven days from the time of the emergency employment, whichever is earliest. 50 U.S.C. §§ 1805(e)(3), 1824(e)(3). Moreover, if no FISC order is issued, absent a showing of good cause, the FISC judge shall cause to be served on any United States person named in the application and on such other United States persons subject to electronic surveillance as the judge may determine in his discretion it is in the interest of justice, notice of the fact of the application, the period of the surveillance, and the fact that during the period information was or was not obtained. 50 U.S.C. § 1806(j), 50 U.S.C. § 1824(j)(1). 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. 50 U.S.C. §§ 1805(e)(5), 1824(e)(5).

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

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

> (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) 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); *see also* 50 U.S.C. § 1821(1) (adopting the definitions from 50 U.S.C. § 1801). With the exception of emergency authorizations, FISA requires that a court order be obtained before any electronic surveillance or physical search may be conducted.

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;
>
> (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 subjected to the surveillance;
>
> (6) a certification, discussed below, of a high-ranking official;
>
> (7) a summary of the manner or means by which the electronic surveillance 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, or places specified in the application; and
>
> (9) the proposed duration of the electronic surveillance.

50 U.S.C. § 1804(a)(1)-(9).

An application to conduct physical search pursuant to FISA must contain similar information as an application to conduct electronic surveillance except that an application to conduct physical search must also contain a statement of the facts and circumstances that justify an applicant's belief that "the premises or property to be searched contains foreign intelligence information" and that the "premises or property to be searched is or is about to be, owned, used, possessed by, or is in transit to or from" the target. 50 U.S.C. §§ 1823(a)(1)-(8), (a)(3)(B), (C).

1. <u>The Certification</u>

An application to the FISC for a FISA order 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)(6); *see also* 50 U.S.C. § 1823(a)(6).

2. Minimization Procedures

The Attorney General has adopted, and the FISC has approved, minimization procedures that regulate the acquisition, retention, and dissemination of non-publicly available information concerning unconsenting United States persons obtained through FISA-authorized electronic surveillance or physical search, including persons who are not the targets of the FISA authorities. 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) (electronic surveillance), 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), 1821(4)(c).

[CLASSIFIED MATERIAL REDACTED].

3. Attorney General's Approval

FISA further requires that the Attorney General 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 and/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 are being used, or are about to be used, by a foreign power or an agent of a foreign power, or that the premises or property to be searched is, or is about to be, 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 section 1801(h) (electronic surveillance) and section 1821(4) (physical search);

(4) the application contains all of the statements and certifications required by section 1804 (electronic surveillance) or section 1823 (physical search); and

(5) if the target is a United States person, the certifications are not clearly erroneous.

50 U.S.C. §§ 1805(a)(1)-(4), 1824(a)(1)-(4).

FISA defines "foreign power" to mean –

(1) a foreign government or any component, thereof, whether or not recognized by the United States;

(2) a faction of a foreign nation or nations, not substantially composed of United States persons;

(3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;

(4) a group engaged in international terrorism or activities in preparation therefor;

(5) a foreign-based political organization, not substantially composed of United States persons;

(6) an entity that is directed and controlled by a foreign government or governments; or

(7) an entity not substantially composed of United States persons that are engaged in the international proliferation of weapons of mass destruction.

50 U.S.C. § 1801(a)(1)-(7); *see also* 50 U.S.C. § 1821(1) (adopting definitions from 50 U.S.C. § 1801).

"Agent of a foreign power" means –

(1) any person other than a United States person, who—

(A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4);

(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities;

(C) engages in international terrorism or activities in preparation therefor [sic];

(D) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor; or

(E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor for or on behalf of a foreign power; or

(2) any person who –

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

> (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;
>
> (D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or
>
> (E) knowingly aids or abets any person in the conduct of activities described in subparagraphs (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraphs (A), (B), or (C).

50 U.S.C. § 1801(b)(1) and (2); *see also* 50 U.S.C. § 1821(1) (adopting definitions from 50 U.S.C. § 1801).

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). Although protected First Amendment activities cannot form the sole basis for FISA-authorized electronic surveillance or physical search, they may be considered by the FISC if there is other activity indicating that the target is an agent of a foreign power. *United States v. Rahman*, 861 F. Supp. 247, 252 (S.D.N.Y. 1994), *aff'd*, 189 F.3d 88 (2d Cir. 1999); *United States v. Rosen*, 447 F. Supp. 2d 538, 548-49 (E.D. Va. 2006). The FISA application must establish probable cause to believe the target is acting as an agent of a foreign power at the time of the application. *See United States v. Abu-Jihaad*, 531 F. Supp. 2d 299, 310 (D. Conn. 2008) (finding that the FISA collection was lawfully collected and finding specifically, *inter alia*, that "[e]ach application contained facts establishing probable cause to believe that, at the time the application was submitted to the FISC, the target of the FISA collection was an agent of a foreign power . . . ."), *aff'd*, 630 F.3d 102, 129 (2d Cir. 2010); *United States v. Squillacote*, 221 F.3d 542, 554 (4th Cir.

2000) (concluding that the FISA applications established "probable cause to believe that . . . [the targets] were agents of a foreign power at the time the applications were granted); *Global Relief Found. Inc. v. O'Neill*, 207 F. Supp. 2d 779, 790 (N.D. Ill. 2002) (concluding that "the FISA application established probable cause . . . at the time the search was conducted and the application was granted"), *aff'd* 315 F.3d 748 (7th Cir. 2002). However, 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 has made all of the necessary findings and is satisfied that the FISA application meets the statutory provisions, the FISC issues an *ex parte* order authorizing the electronic surveillance, physical search, or both, requested in the application. 50 U.S.C. §§ 1805(a), 1824(a). The order must specify:

> (1) the identity, if known, 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 manner and 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), (2)(A), 1824(c)(1), (2)(A).

Under FISA, electronic surveillance or physical search targeting a United States person may be approved for up to 90 days, and those targeting a non-United States person may be approved for up to 120 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. An extension for electronic surveillance or physical search targeting a United States person may be approved for up to 90 days, and one targeting a non-United States person may be approved for up to one year.[12] 50 U.S.C. §§ 1805(d)(2), 1824(d)(2).

III. DISTRICT COURTS' REVIEW OF FISC ORDERS

FISA authorizes the use in a criminal prosecution of information obtained or derived from any FISA-authorized electronic surveillance or physical search, provided that advance authorization is obtained from the Attorney General, 50 U.S.C. §§ 1806(b), 1825(c), and that proper notice is subsequently given to the court and to each aggrieved person against whom the information is to be used. 50 U.S.C. §§ 1806(c)-(d), 1825(d)-(e). Under Section 1806(c), the government's notice obligation applies only if the government "intends to enter into evidence or otherwise use or disclose" (2) against an "aggrieved person" [13] (3) in a "trial, hearing or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States" (4) any "information obtained or derived from" (5) an "electronic surveillance [or physical search] of that aggrieved person." 50 U.S.C. § 1806(c); *see* 50 U.S.C.

[12] The FISC retains the authority to review, before the end of the authorized period of electronic surveillance or physical search, the Government's compliance with the requisite minimization procedures. 50 U.S.C. §§ 1805(d)(3), 1824(d)(3).

[13] 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).

§ 1825(d). Upon receiving notice, an aggrieved person against whom the information is to be used may move to suppress the use of the FISA information on two grounds:[14] (1) the information was unlawfully acquired; or (2) the electronic surveillance or physical search was not conducted in conformity with an order of authorization or approval. 50 U.S.C. §§ 1806(e), 1825(f). In addition, FISA contemplates that a defendant may file a motion or request under any other statute or rule of the United States to discover or obtain applications, orders, or other materials relating to electronic surveillance or physical search, *i.e.*, the FISA materials. 50 U.S.C. §§ 1806(f), 1825(g). When a defendant moves to suppress FISA information under 50 U.S.C. §§ 1806(e) or 1825(f), or seeks to discover the FISA materials under some other statute or rule, the motion or request is evaluated using FISA's probable cause standard, which is discussed below, and not the probable cause standard applicable to criminal warrants. *See, e.g.*, *United States v. El-Mezain*, 664 F.3d 467, 564 (5th Cir. 2011); *United States v. Duka*, 671 F.3d 329, 336-37 (3d Cir. 2011) (rejecting appellant's challenge to FISA's probable cause standard because it does not require any indication that a crime has been committed).

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

In assessing the legality of FISA-authorized electronic surveillance and physical search, the district court:

> shall, notwithstanding any other law, if the Attorney General files 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 [or search] as may be necessary to determine whether the surveillance [or search] of the aggrieved person was lawfully authorized and conducted.[15]

---

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

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

50 U.S.C. §§ 1806(f), 1825(g). On the filing of the Attorney General's affidavit or declaration, such as has been filed here, 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). Thus, the propriety of the disclosure of any FISA applications or orders to a defendant may not 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 acquired collection after reviewing the Government's submissions (and any supplemental pleadings that the district court may request) *in camera* and *ex parte*. *See Abu-Jihaad*, 630 F.3d at 129 (concluding that "disclosure of FISA materials 'is the exception and *ex parte*, *in camera* determination is the rule'") (quoting *United States v. Stewart*, 590 F.3d 93, 129 (2d Cir. 2009)); *El-Mezain*, 664 F.3d at 565 (quoting 50 U.S.C. § 1806(f)); *United States v. Belfield*, 692 F.2d 141, 147 (D.C. Cir. 1982).

If the district court is able to make an accurate determination of the legality of the electronic surveillance and/or physical search 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 Abu-Jihaad,* 630 F.3d at 129 (quoting 50 U.S.C. § 1806(g)); *El-Mezain*, 664 F.3d at 566.

1. *In Camera, Ex Parte* Review Is Required Under FISA

Federal courts, including those in the Second Circuit, have repeatedly and consistently held that FISA anticipates an "*ex parte*, *in camera* determination is to be the rule," *United States v. Duggan*, 743 F.2d 59, 78 (2d Cir. 1984) (quoting *Belfield*, 692 F.2d at 147), with disclosure

and an adversarial hearing being the "exception, occurring *only* when necessary."[16] *United States v. Omar*, 786 F.3d 1104, 1110 (8th Cir. 2015) (citing *United States v. Isa*, 923 F.2d 1300, 1306 (8th Cir. 1991)); *see also* Dec. 29, 2016, Tr. 20:17-21:21:15, *United States v. Gammal*, No. 15 Cr. 588 (E.R.) (S.D.N.Y.) (hereinafter, "*Gammal*") (attached as Ex. A). In fact, every court but one (whose decision was subsequently overturned by an appellate court)[17] that has addressed a motion to disclose FISA materials or to suppress FISA information has been able to reach a conclusion as to the legality of the FISA collection at issue based on its *in camera, ex parte* review. *See, e.g.*, *Gammal*, at Ex. A, 21:16-21; *see also Stewart*, 590 F.3d at 128 ("'[*E*]*x parte, in camera* determination is to be the rule'" (quoting *Belfield*, 692 F.2d at 147)); *El-Mezain*, 664 F.3d at 566-67 (quoting district court's statement that no court has ever held an adversarial hearing to assist the court); *In re Grand Jury Proceedings of the Special Apr. 2002 Grand Jury* ("*In re Grand Jury Proceedings*"), 347 F.3d 197, 203 (7th Cir. 2003) (noting that no court had ever ordered disclosure of FISA materials); *United States v. Medunjanin*, No. 10 Cr 191 (RJD), 2012 WL 526428, at *10 (E.D.N.Y. Feb. 16, 2012) (noting that "[n]o United States District Court or Court of Appeals has ever determined that disclosure to the defense of such materials

---

[16] In *Duggan*, the Second Circuit explained that disclosure might be necessary if the judge's initial review revealed potential irregularities such as 'possible misrepresentations of fact, vague identification of persons to be surveilled or surveillance records which include a significant amount of nonforeign intelligence information, calling into question compliance with the minimization standards contained in the order. 743 F.2d at 78 (quoting S. Rep. 95-604, at 58 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3960).

[17] In *United States v. Daoud*, the district court ruled that it was capable of making the determination, but nevertheless ordered the disclosure of FISA materials to the defense. No. 12 Cr 723, 2014 WL 321384, at *8 (N.D. Ill. Jan. 29, 2014). The Government appealed the *Daoud* court's order to the U.S. Court of Appeals for the Seventh Circuit, which overturned the district court's decision to disclose FISA materials, stating, "[s]o clear is it that the materials were properly withheld from defense counsel that there is no need for a remand to enable the district judge to come to the same conclusion, because she would have to do so." *United States v. Daoud*, 755 F.3d 479, 485 (7th Cir. 2014).

was necessary to determine the lawfulness of surveillance or searches under FISA" (quoting *United States v. Warsame*, 547 F. Supp. 2d 982, 987 (D. Minn. 2008))); *Abu-Jihaad*, 531 F. Supp. 2d at 310 ("Courts have uniformly held that *ex parte* and *in camera* inspections are the 'rule' under FISA. . . ." (citing *Duggan*, 743 F. 2d at 78)); *United States v. Thomson,* 752 F. Supp. 75, 77 (W.D.N.Y. 1990) (noting that no court "has found disclosure or an adversary hearing necessary"); *United States v. Sattar*, No. 02-Cr-395 JGK, 2003 WL 22137012, at *6 (S.D.N.Y. Sept. 15, 2003) (noting "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" (citing *United States v. Nicholson*, 955 F. Supp. 588, 592 & n.11 (E.D. Va. 1997))).

As the exhibits in the Sealed Appendix make clear, there is nothing extraordinary about the FISA-authorized electronic surveillance and physical search in this case that would justify the production and disclosure of highly sensitive and classified FISA materials or the suppression of FISA-obtained or -derived evidence. Here, the FISA materials are well-organized and easily reviewable by the Court *in camera* and *ex parte*, and they are fully and facially sufficient to allow the Court to make an accurate determination that the FISA information was lawfully acquired and that the electronic surveillance and physical search were made in conformity with an order of authorization or approval. In other words, the materials presented "are straightforward and readily understood." *In re Kevork*, 634 F. Supp. 1002, 1008 (C.D. Cal. 1985), *aff'd*, 788 F.2d 566 (9th Cir. 1986); *see also Gammal*, at Exhibit A, 21:16-21. Moreover, as in other cases, "[t]he determination of legality in this case is not complex." *Belfield*, 692 F.2d at 147; *see also United States v. Hasbajrami*, No. 11-CR-623 (JG), 2016 WL 1029500, at *14 (E.D.N.Y. Feb. 18, 2016) (finding the review of the FISA materials was "relatively straightforward and not complex" such that the court "was able to evaluate the legality of the

challenged surveillance without concluding that due process first warranted disclosure") (internal quotations and citations omitted); *Warsame*, 547 F. Supp. 2d at 987 (finding that the "issues presented by the FISA applications are straightforward and uncontroversial"); *Abu-Jihaad*, 531 F. Supp. 2d at 310; *Thomson*, 752 F. Supp. at 79. This Court, much like the aforementioned courts, is capable of reviewing the FISA materials *in camera* and *ex parte* and making the requisite legal determination without an adversarial hearing.

In addition to the specific harm that would result from the disclosure of the FISA materials in this case, which is detailed in the classified declaration of an Assistant Director of the FBI in support of the Attorney General's Declaration and Claim of Privilege, 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." *United States v. Ott*, 637 F. Supp. 62, 65 (E.D. Cal. 1986), *aff'd*, 827 F.2d 473 (9th Cir. 1987); *accord Isa*, 923 F.2d at 1306 (the Court's "study of the materials leaves no doubt that substantial national security interests required the *in camera*, *ex parte* review, and that the district court properly conducted such a review"); *Medunjanin*, 2012 WL 526428, at *9 (finding persuasive the Government's argument that "unsealing the FISA materials in this case would provide the defense with unnecessary details of an extraordinarily sensitive anti-terrorism investigation").

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. . . ." *Central Intelligence Agency v. Sims*, 471 U.S. 159, 175 (1985). When considering 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, if 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. Central Intelligence Agency*, 629 F.2d 144, 150 (D.C. Cir. 1980) (noting that "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"); *Medunjanin*, 2012 WL 526428, at *10 (quoting *Yunis*, 867 F.2d at 625). An adversary hearing is not only unnecessary to aid the Court in the straightforward task before it, but such a hearing would also create potential dangers that courts have consistently sought to avoid.

As the Second Circuit explained in *Stewart*:

> FISA applications are likely to contain allegedly sensitive information relating to perceived issues of national security. The applications are required to set forth how and why the Executive Branch knows what it knows, which may include references to covert agents and informers. For this reason, *ex parte*, *in camera* determination is to be the rule.

590 F.3d at 128 (quoting *Duggan*, 743 F.2d at 77).

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

The constitutionality of FISA's *in camera, ex parte* review provisions has been affirmed by every federal court that has considered the matter, including the Second Circuit and the

Southern District of New York. *See, e.g, Gammal*, at Exhibit A, 21:16-21, 22:18-22; *see also Abu-Jihaad*, 630 F.3d at 129 (affirming district court's determination that "its *in camera, ex parte* review permitted it to assess the legality of the challenged surveillance and the requirements of due process did not counsel otherwise"); *Stewart*, F.3d 590 at 126 (noting that "the procedures fashioned in FISA [are] a constitutionally adequate balancing of the individual's Fourth Amendment rights against the nation's need to obtain foreign intelligence information." (quoting *Duggan*, 743 F. 2d at 73)); *United States v. Fishenko*, No. 12 Civ. 626 (SJ), 2014 WL 8404215, at *7 (E.D.N.Y. Sept. 25, 2014) (citing numerous decisions by U.S. district courts in the Second Circuit and concluding that "there is no question as to the constitutionality of FISA"); *United States v. Sattar*, 2003 WL 22137012, , at *5-6; *accord Duka*, 671 F.3d at 337 (rejecting the defendant's constitutional challenge to the use of FISA-derived evidence at trial, thereby "[a]ligning with all of the other courts of appeals that have considered this issue"); *El-Mezain*, 664 F.3d at 567 (agreeing with district court that its *in camera, ex parte* review ensured the defendant's constitutional and statutory rights were not violated); *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"); *ACLU Found. of S. Cal. v. Barr*, 952 F.2d 457, 465 (D.C. Cir. 1991) (procedure under FISA "is an acceptable means of adjudicating the constitutional rights of persons who have been subjected to FISA surveillance" (citing *Belfield*, 692 F.2d at 141)); *Ott*, 827 F.2d at 476-77 (FISA's review procedures do not deprive a defendant of due process).

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 to determine whether the FISA information was lawfully acquired and whether the electronic surveillance and

physical search were made in conformity with an order of authorization or approval. *In camera, ex parte* review is the rule in such cases, and that procedure 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. Accordingly, an *in camera, ex parte* review by this Court is the appropriate method to determine whether the FISA information was lawfully acquired and whether the electronic surveillance and physical search were conducted in conformity with an order of authorization or approval.

B. THE DISTRICT COURT'S SUBSTANTIVE REVIEW

1. Standard of Review of Probable Cause

In evaluating the legality of the FISA collection, a district court's review should determine: (1) whether the certification submitted by the Executive Branch in support of a FISA application was properly made; (2) whether the application established the probable cause showing required by FISA; and (3) whether the collection was properly minimized. *See Abu-Jihaad*, 630 F.3d at 130-31; *see also* 50 U.S.C. §§ 1806(a), (f), 1824(a), 1825(g).

Although federal courts are not in agreement as to whether the FISC's probable cause determination should be reviewed *de novo* or afforded due deference, courts in the Second Circuit have afforded due deference to the determinations of the FISC.[18] *See Gammal*, at Exhibit A, 22:23-23:8; *see also Abu-Jihaad*, 630 F.3d at 130; *Stewart*, 590 F.3d at 128; *Hasbajrami*,

[18] Federal courts in other circuits have determined that the probable cause determination of the FISC should be reviewed *de novo*. *See United States v. Hammoud*, 381 F.3d 316, 332 (4th Cir. 2004), *rev'd on other grounds*, 543 U.S. 1097 (2005), *op. reinstated in pertinent part*, 405 F.3d 1034 (4th Cir. 2005); *Rosen*, 447 F. Supp. 2d at 545; *Warsame*, 547 F. Supp. 2d at 990-91; *United States v. Kashmiri*, No. 09 Cr 830-4, 2010 WL 4705159, at *1 (N.D. Ill. Nov. 10, 2010); *United States v. Nicholson*, No. 09-Cr-40-BR, 2010 WL 1641167, at *5 (D. Or. Apr. 20, 2010). In each of these cases, the courts applied a *de novo* standard in reviewing the FISC's probable cause findings, and each court found that applications before it contained probable cause.

2016 WL 1029500, at *13; *Fishenko*, 2014 WL 8404215, at *8; *cf Medunjanin*, 2012 WL 526428, at *6-7 (affording deferential review, but noting that such review is not superficial).

2. Probable Cause Standard

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 place at which the electronic surveillance is directed is being used, or is about to be used, or that the property or premises to be searched is, or is about to be, owned, used, possessed by, or is in transit to or from, a foreign power or an agent of a foreign power. 50 U.S.C. §§ 1805(a), 1824(a); *Abu-Jihaad*, 630 F.3d at 130; *see also Gammal*, at Exhibit A, 23:10-16. It is this standard – not the standard applicable to criminal search warrants – that this Court must apply. *Medunjanin*, 2012 WL 526428, at *6 ("[N]o branch of government – whether executive or judicial – need make a probable cause finding of *actual or potential* criminal activity to justify a FISA warrant"); *El-Mezain*, 664 F.3d at 564; *United States v. Cavanagh*, 807 F.2d 787, 790 (9th Cir. 1987) (citing *United States v. United States District Court (Keith)*, 407 U.S. 297, 322 (1972)).

The probable cause showing the Government must satisfy before receiving authorization to conduct electronic surveillance or physical search under FISA complies with the Fourth Amendment's reasonableness standard. The argument that FISA's different probable cause standard violates the Fourth Amendment's reasonableness requirement has been uniformly rejected by federal courts. *See, e.g.*, *Abu-Jihaad*, 630 F.3d at 120 (rejecting the defendant's Fourth Amendment claim and listing 16 cases that stand for the proposition that FISA does not violate the Fourth Amendment).

[CLASSIFIED MATERIAL REDACTED].

3. Standard of Review of Certifications

Certifications submitted in support of a FISA application should be "subjected to only minimal scrutiny by the courts," and are "presumed valid." *Duggan*, 743 F.2d at 77 & n.6 (citing *Franks v. Delaware*, 438 U.S. 154, 171 (1978)); *United States v. Campa*, 529 F.3d 980, 993 (11th Cir. 2008) (quoting *United States v. Badia*, 827 F.2d 1458, 1463 (11th Cir. 1987)); *United States v. Sherifi*, 793 F. Supp. 2d 751, 760 (E.D.N.C. 2011); *Warsame*, 547 F. Supp. 2d at 990. 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. A district court's review should determine whether the certifications were made in accordance with FISA's requirements. 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.*; *Rahman*, 861 F. Supp. at 250 (citing *Duggan*); *Omar*, 2012 WL 2357734, at *3 ("The reviewing court must presume as valid 'the representations and certifications submitted in support of an application for FISA surveillance' . . . absent a showing sufficient to trigger a *Franks* hearing." (quoting *Duggan*, 743 F. 2d at 77)); *In re Grand Jury Proceedings*, 347 F.3d at 204-05; *Badia*, 827 F.2d at 1463; *Kashmiri*, 2010 WL 4705159, at *1; *United States v. Islamic Am. Relief Agency (IARA)*, No. 07-87-Cr-NKL), 2009 WL 5169536, at *4 (W.D. Mo. Dec. 21, 2009). When the target is a United States person, the district court should also ensure that each certification is not "clearly erroneous." *Duggan*, 743 F.2d at 77; *Campa*, 529 F.3d at 994; *Kashmiri*, 2010 WL 4705159, at *2. A "clearly erroneous" finding is established 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. Garcia*, 413 F.3d 201, 222 (2d Cir. 2005) (quoting *U.S. Gypsum Co.*, 333 U.S. at 395).

4. FISA Is Subject to the "Good-Faith" Exception

Even assuming *arguendo* that 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 met, the evidence obtained or derived from the FISA-authorized electronic surveillance and physical search is, nonetheless, admissible under the "good faith" exception to the exclusionary rule articulated in *United States v. Leon*, 468 U.S. 897 (1984). *See United States v. Ahmed*, No. 06-Cr-147-(WSD)-(GGB), 2009 U.S. Dist. LEXIS 120007, at *25 n.8, 26-27 (N.D. Ga. Mar 19, 2009) (noting that federal officers are entitled to rely in good faith on a FISA warrant (citing *United States v. Ning Wen*, 477 F.3d 896, 897 (7th Cir. 2007)).

The FISA-authorized electronic surveillance and physical search at issue in this case, authorized by a duly enacted statute and an order issued by a neutral judicial officer, would fall squarely within this good faith exception. There is no basis to find that any declarations or certifications at issue in this case were deliberately or recklessly false. *See Leon*, 468 U.S. at 914-15; *Massachusetts v. Sheppard*, 468 U.S. 981, 987-88 (1984). Further, there are no facts indicating that the FISC failed to act in a neutral and detached manner in authorizing the electronic surveillance and physical search at issue. *See Leon*, 468 U.S. at 914-15. Moreover, as the Court will see from its *in camera, ex parte* review of the FISA materials, facts establishing the requisite probable cause were submitted to the FISC, the FISC's orders contained all of the requisite findings, and "well-trained officers" reasonably relied on those orders. Therefore, in the event that the Court questions whether a particular FISC order was supported by sufficient

probable cause, the information obtained pursuant to that order would be admissible under *Leon*'s "good faith" exception to the exclusionary rule.

IV. THE FISA INFORMATION WAS LAWFULLY ACQUIRED AND THE ELECTRONIC SURVEILLANCE AND PHYSICAL SEARCH WERE MADE IN CONFORMITY WITH AN ORDER(S) OF AUTHORIZATION OR APPROVAL

[CLASSIFIED MATERIAL REDACTED].

A. THE INSTANT FISA APPLICATION(S) MET FISA'S PROBABLE CAUSE STANDARD

[CLASSIFIED MATERIAL REDACTED].

1. [CLASSIFIED MATERIAL REDACTED].

[CLASSIFIED MATERIAL REDACTED].

2. [CLASSIFIED MATERIAL REDACTED].

[CLASSIFIED MATERIAL REDACTED].

a. [CLASSIFIED MATERIAL REDACTED].

[CLASSIFIED MATERIAL REDACTED].

b. [CLASSIFIED MATERIAL REDACTED].

[CLASSIFIED MATERIAL REDACTED].

c. [CLASSIFIED MATERIAL REDACTED].

[CLASSIFIED MATERIAL REDACTED].

d. [CLASSIFIED MATERIAL REDACTED].

[CLASSIFIED MATERIAL REDACTED

e. [CLASSIFIED MATERIAL REDACTED].

[CLASSIFIED MATERIAL REDACTED].

f. [CLASSIFIED MATERIAL REDACTED].

[CLASSIFIED MATERIAL REDACTED].

g. [CLASSIFIED MATERIAL REDACTED].

[CLASSIFIED MATERIAL REDACTED].

h. [CLASSIFIED MATERIAL REDACTED].

[CLASSIFIED MATERIAL REDACTED].

i. [CLASSIFIED MATERIAL REDACTED].

[CLASSIFIED MATERIAL REDACTED].

j. [CLASSIFIED MATERIAL REDACTED].

[CLASSIFIED MATERIAL REDACTED].

k. [CLASSIFIED MATERIAL REDACTED].

[CLASSIFIED MATERIAL REDACTED].

3. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED].

a. [CLASSIFIED MATERIAL REDACTED].

[CLASSIFIED MATERIAL REDACTED].

***i.* [CLASSIFIED MATERIAL REDACTED].**

[CLASSIFIED MATERIAL REDACTED].

***ii.* [CLASSIFIED MATERIAL REDACTED].**

[CLASSIFIED MATERIAL REDACTED].

***iii.* [CLASSIFIED MATERIAL REDACTED].**

[CLASSIFIED MATERIAL REDACTED].

***iv.* [CLASSIFIED MATERIAL REDACTED].**

[CLASSIFIED MATERIAL REDACTED].

b. Conclusion: There Was Sufficient Probable Cause to Establish that the Information Acquired from the Targeted Facility(ies), Place(s), Property, or Premises Was Lawfully Acquired

[CLASSIFIED MATERIAL REDACTED].

B. THE CERTIFICATIONS COMPLIED WITH FISA

[CLASSIFIED MATERIAL REDACTED].

1. Foreign Intelligence Information

[CLASSIFIED MATERIAL REDACTED].

2. "A Significant Purpose"

[CLASSIFIED MATERIAL REDACTED].

3. Information Not Reasonably Obtainable Through Normal Investigative Techniques

[CLASSIFIED MATERIAL REDACTED].

C. THE ELECTRONIC SURVEILLANCE AND PHYSICAL SEARCH WERE CONDUCTED IN COMFORMITY WITH AN ORDER OF AUTHORIZATION OF APPROVAL

[CLASSIFIED MATERIAL REDACTED].

1. The Minimization Procedures

Once a reviewing court is satisfied that the FISA information was lawfully acquired, it must then examine whether the electronic surveillance and physical search were lawfully conducted. *See* 50 U.S.C. §§ 1806(e)(2), 1825(f)(1)(B). In order to examine whether the electronic surveillance or physical search were lawfully conducted, the reviewing court must determine whether the Government followed the relevant minimization procedures to appropriately minimize the information acquired pursuant to FISA.

[CLASSIFIED MATERIAL REDACTED].

FISA's legislative history and the applicable case law demonstrate that the definitions of "minimization procedures" and "foreign intelligence information" were intended to take into account the realities of collecting foreign intelligence because the activities of persons engaged in clandestine intelligence gathering or international terrorism are often not obvious on their face. The degree to which information is required to be minimized varies somewhat given the specifics of a particular investigation, such that less minimization at acquisition 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. 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, organization, activities and plans. *See, e.g., United States v. Salameh*, 152 F.3d 88, 154 (2d Cir. 1998) (noting that two 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]innocuous-sounding conversations may in fact be signals of important activity; information on its face innocent when analyzed or considered with other information may become critical." *Kevork*, 634 F. Supp. at 1017 (quoting H.R. Rep. No. 95-1283, pt. 1, at 55 (1978)); *see also Hammoud*, 381 F.3d at 334 (citing *Salameh*, 152 F.3d at 154); *In re Sealed Case*, 310 F.3d at 740-41; *United States v. Bin Laden*, 126 F. Supp. 2d 264, 286 (S.D.N.Y. 2000). One court recognized that "the Congress that enacted FISA observed that 'bits and pieces of information, which taken separately could not possibly be considered "necessary" may together over time take on significance.'" *Medunjanin*, 2012 WL 526428, at *4

(quoting H.R. Rep. No. 95-1283, pt. 1, at 58-59). As a result, "courts have construed 'foreign intelligence information' broadly and sensibly allowed the government some latitude in its determination of what is foreign intelligence information." *Rosen*, 447 F. Supp. 2d at 551.

The nature of the foreign intelligence information sought also impacts implementation of the minimization procedures at the retention and dissemination stages. 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. As Congress explained:

> 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 persons 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.

H.R. Rep. No. 95-1283, pt. 1, at 58. Indeed, at least one court has 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. 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.* at 81-82 (quoting H.R. Rep. No. 1283, pt. 1, at 59).

In light of these realities, Congress recognized that "no electronic surveillance can be so conducted that innocent conversations can be totally eliminated." *See* S. Rep. No. 95-701, at 39

(1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4008 (quoting *United States v. Bynum,* 485 F.2d 490, 500 (2d Cir. 1973)). The Fourth Circuit reached the same conclusion in *Hammoud*, stating that the "mere fact that innocent conversations were recorded, without more, does not establish that the government failed to appropriately minimize surveillance." 381 F.3d at 334; *see also United States v. Goffer*, 756 F. Supp. 2d 588, 592 (S.D.N.Y. 2011) (referencing Title III wiretap surveillance).

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). "The test of compliance is 'whether a good-faith effort to minimize was made.'" *United States v. Mubayyid*, 521 F. Supp. 2d 125, 135 (D. Mass. 2007); *see also Hammoud*, 381 F.3d at 334 ("The minimization requirement obligates the Government to make a good faith effort to minimize the acquisition and retention of irrelevant information." (citing S. Rep. No. 95-701, at 39-40 (1978))); *Hasbajrami*, 2016 WL 1029500, at *14 (quoting *Mubayyid*); *Sattar*, 2003 WL 22137012, at *10-11; S. Rep. No. 95-701, at 39-40, 1978 U.S.C.C.A.N., at 4008-09 (stating that the court's role is to determine whether "on the whole, the agents have shown a high regard for the right of privacy and have done all they reasonably could do to avoid unnecessary intrusion").

Moreover, as noted above, 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), 1821(4)(c); *see also Isa*, 923 F.2d at 1304 (noting that

"[t]here is no requirement that the 'crime' be related to foreign intelligence"). As a result, to the extent that certain communications of a United States person may be evidence of a crime or otherwise may establish an element of a substantive or conspiratorial offense, such communications need not be minimized. *See id.* at 1305.

Assuming, for the sake of argument, that certain communications were not minimized in accordance with the SMPs, suppression would not be the appropriate remedy with respect to those communications that met the standard. *Cf. 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). As discussed above, absent evidence that "on the whole" there has been a "complete" disregard for the minimization procedures, the fact that some communications should have been minimized does not affect the admissibility of others that were properly acquired and retained. FISA's legislative history reflects that Congress intended only a 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.

H.R. Rep. No. 1283, pt. 1, at 93; *see also Falcone*, 364 F. Supp. at 886-87; *Medunjanin*, 2012 WL 526428, at *12 (disclosure and suppression not warranted where "failure to adhere to [the minimization] protocol was *de minimis*").

2. The FISA Information Was Appropriately Minimized

[CLASSIFIED MATERIAL REDACTED].

Based upon this information, we respectfully submit that the Government lawfully conducted the FISA collection discussed herein. Consequently, for the reasons stated above, the Court should find that the FISA collection discussed herein was lawfully conducted under the

minimization procedures approved by the FISC and applicable to the FISA collection discussed herein.[19]

V. THE COURT SHOULD REJECT THE DEFENDANT'S LEGAL ARGUMENTS

The defendant's motions seek the following: (1) suppression of the FISA information; (2) in the alternative, a *Franks* hearing relating to the suppression motion that would entail disclosure of the FISA materials; and (3) notice and discovery of any E.O. 12333 information used in the instant criminal proceedings. (Docs. 60 and 61 at 1.) For the reasons set forth below and as the Court will see in its *ex parte*, *in camera* review of the FISA materials, the defendant's arguments are without merit.

A. THE DEFENDANT HAS NOT ESTABLISHED ANY BASIS FOR THE COURT TO SUPPRESS THE FISA INFORMATION

[CLASSIFIED MATERIAL REDACTED].

1. The Government Satisfied the Probable Cause Requirements of FISA

The defendant asserts that he was acting "on his own or at the behest of law enforcement officers" and that there was no probable cause to believe that he was an "'agent of a foreign power 'acting 'for or on behalf of a foreign power. '" (Doc. 60 at 6-9). Probable cause, while more than a bare suspicion, is "less than absolute certainty," and in making the probable cause determination, FISA permits a judge to "consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target." *Rosen*, 477 F.Supp. 2d at 549 (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983)); 50 U.S.C. § 1805(b). Furthermore, the FISA probable cause standard "does not necessarily require a showing of an imminent violation of criminal law" because Congress clearly intended a different showing of probable cause for

[19] **[CLASSIFIED MATERIAL REDACTED].**

these activities than that applicable to ordinary cases. *Rosen*, 477 F.Supp. 2d at 549 (citing *In re Sealed Case*, 310 F.3d. at 739). As discussed above, courts in the Second Circuit have afforded due deference to the probable cause determinations of the FISC. *See Abu-Jihaad*, 630 F.3d at 130; *Stewart*, 590 F.3d at 128; *Hasbajrami*, 2016 WL 1029500, at *13; *Fishenko*, 2014 WL 8404215, at *8; *cf. Medunjanin*, 2012 WL 526428, at *6-7 (affording deferential review, but noting that such review is not superficial). Here, a review of the FISA materials shows that the Government plainly satisfied the requirements of FISA.

[CLASSIFIED MATERIAL REDACTED].

The defendant also claims that the Government's probable cause showing may have been based solely on his conversations with "ISIL operatives or sympathizers or [those who] expressed support for ISIL" and his possession of "ISIL flags and videos," which are activities protected by the First Amendment of United States Constitution. (Doc. 60, at 9-11). Contrary to the defendant's claim, not all speech- or advocacy-related activities fall within the protection of the First Amendment. For instance, conversations with co-conspirators merit no First Amendment protection because they are statements made in furtherance of a conspiracy and are evidence of the participant's criminal intent. "Numerous crimes under the federal criminal code are, or can be, committed by speech alone . . . . [I]f the evidence shows that the speech crossed the line into criminal solicitation, procurement of criminal activity, or conspiracy to violate the laws, the prosecution is permissible." *United States v. Rahman*, 189 F.3d 88, 117 (2d Cir. 2008); *United States v. Sattar*, 395 F. Supp. 2d 79, 101 (S.D.N.Y. 2005) ("First Amendment lends no protection to participation in conspiracy, even if such participation is through speech"); *see also United States v. Moldanado-Rivera*, 922 F.2d 934, 962 (2d Cir. 1990), (conspirators statements are admissible even where no conspiracy offense is charged), *cert. denied,* 501 U.S. 1233 (1991).

[CLASSIFIED MATERIAL REDACTED].

2. The Certifications Complied with FISA

The defendant also claims that there may be defects in the certifications included in the FISA application(s). Specifically, the defendant argues that the application(s) fail to demonstrate that the gathering of foreign intelligence information was a "significant purpose" of the FISA orders. (Doc. 60 at 11-12.) Additionally, the defendant implies that the certification that the information could not have been obtained through normal investigative techniques was incorrect. (Doc. 60 at 13.)

[CLASSIFIED MATERIAL REDACTED].

3. The Government Legally Conducted FISC-Authorized Electronic Surveillance and Physical Search

[CLASSIFIED MATERIAL REDACTED].

4. The Government Complied with the Minimization Procedures

[CLASSIFIED MATERIAL REDACTED].[20]

The Government respectfully submits that the Court's *ex parte*, *in camera* review of the FISA materials will demonstrate that the Government complied with all of FISA's statutory requirements. Accordingly, the Government submits that there is no basis to suppress the FISA information in the present case.

[20] The defendant's reliance on the FISC opinion made public in redacted form on April 26, 2017 ("April 2017 FISC Op."), is misplaced. (Doc. 60 at 15-16). That opinion addresses only "upstream" information collected from non-U.S. persons pursuant to 50 U.S.C. § 1881a.

B. *FRANKS v. DELAWARE* DOES NOT REQUIRE AN EVIDENTIARY HEARING REGARDING THE SUPRESSION OF FISA MATERIALS AND THE DEFENDANT HAS NOT ESTABLISHED ANY BASIS FOR DISCLOSURE OF THE FISA MATERIALS

In support of his request for disclosure, the defendant argues that "due process" should prompt disclosure of the FISA materials. (Doc. 60, at 21.) The defendant speculates further that there were "intentional or reckless" omissions in the application(s) submitted to the FISC, in violation of *Franks v. Delaware*, 438 U.S. 154 (1978), and seeks disclosure of the FISA materials based on this speculation. (*See* Doc. 60, at 16-18). The Court's own review of the FISA materials will demonstrate that no such intentional or reckless omissions occurred. The Court must conduct its review of those materials *in camera* and *ex parte*, and disclosure is within the Court's discretion only following that review and only if the Court is unable to determine the legality of the electronic surveillance and physical search without the assistance of defense counsel. 50 U.S.C. §§ 1806(f), 1825(g); *Duggan*, 743 F.2d at 78; *Daoud*, 755 F.3d at 482; *Rosen*, 447 F. Supp. 2d at 546. As this Court will see from its review, the FISA materials are presented in a well-organized and straightforward manner that will allow the Court to make its determination of the lawfulness of the FISA collection without input from defense counsel. *See Abu-Jihaad*, 630 F.3d at 129 (upholding the district court's ruling that disclosure was unnecessary because its *in camera, ex parte* "review of . . . the FISA materials [was] relatively straightforward and not complex," thereby allowing the court to "assess the legality of the challenged surveillance.") (alteration in original).

The defendant is not entitled to the FISA materials for the purpose of challenging the lawfulness of the FISA authorities, as FISA's plain language precludes defense counsel from accessing the classified FISA materials to conduct a fishing expedition. In *Medunjanin*, the Court noted that "[d]efense counsel . . . may not inspect the FISA dockets to construct a better

argument for inspecting the FISA dockets. Such a circular exercise would be patently inconsistent with FISA . . . ." 2012 WL 526428, at *10; *see also Badia*, 827 F.2d at 1462 (rejecting the defendant's request for "disclosure of the FISA application, ostensibly so that he may review it for errors").

The defendant has failed to present any colorable basis for disclosure, as this Court is able to review and make a determination as to the legality of the FISA collection without the assistance of defense counsel. Where, as here, defense participation is not necessary, FISA requires that the FISA materials remain protected from disclosure. Congress's clear intention is that FISA materials should be reviewed *in camera* and *ex parte* and in a manner consistent with the realities of modern intelligence needs and investigative techniques. There is simply nothing extraordinary about this case that would prompt this Court to order the disclosure of highly sensitive and classified FISA materials. *See Rosen*, 447 F. Supp. 2d at 546 (stating that "exceptional nature of disclosure of FISA material is especially appropriate in light of the possibility that such disclosure might compromise the ability of the United States to gather foreign intelligence information effectively" (citing *Belfield*, 692 F.2d at 147).

Although the defendant states that the Court should hold an adversary hearing (a "*Franks* hearing") on the suppression motion, he advances no argument for doing so. (Doc 60, at 16-18.) Based on the relevant case law, this Court should decline to hold such a hearing. To merit a *Franks* hearing, a defendant must make a "concrete and substantial preliminary showing" that the affiant deliberately or recklessly included false statements, or failed to include material information, in the affidavit, and that the resulting misrepresentation was essential to the finding of probable cause. *Franks*, 438 U.S. at 155-56. Courts apply the same standard when a defendant seeks a *Franks* hearing as part of a challenge to FISA collection; to obtain a hearing, a

defendant must "make 'a substantial preliminary showing that a false statement knowingly or intentionally, or with reckless disregard for the truth, was included' in the application and that the allegedly false statement was 'necessary' to the FISA Judge's approval of the application." *Duggan*, 743 F.2d at 77 n.6 (quoting *Franks*, 438 U.S. at 155-56).[21]

Courts have rejected other defendants' attempts to force a *Franks* hearing by positing unsupported speculation to challenge the validity of FISC orders, and this Court should do so here. *See Gammal*, at Exhibit A, 22:16-23:4, 24:17-21; *see also Damrah*, 412 F.3d at 624-25 (holding that the defendant "failed to meet his threshold burden under *Franks*" because his "*Franks* attack was non-specific and unsupported" (internal citations omitted)); *Abu-Jihaad*, 531 F. Supp. 2d at 311 (concluding with "little difficulty" that the "*Franks* standard [was] not even remotely met"); *Mubayyid*, 521 F. Supp. 2d at 131 ("The balance struck under FISA . . . would be substantially undermined if criminal defendants were granted a right of disclosure simply to ensure against the possibility of a *Franks* violation").

In the case at bar, the defendant has failed to carry the burden of establishing the prerequisites for an adversary hearing, and his attempt to obtain disclosure of the FISA materials to meet that burden is unprecedented and runs counter to FISA, *Franks*, and the intent of Congress. For these reasons, the Court should deny the defendant's request for an adversary hearing on his suppression motion. Moreover, the Government respectfully submits that this Court's *in camera*, *ex parte* review of the FISA materials will demonstrate that "an adversary

[21] Even assuming that the defendant offered sufficient proof to show that an affidavit involved false statements or omissions, a hearing should not be held where the affidavit would still provide probable cause if the allegedly false material were eliminated, or if the allegedly omitted information were included. *Franks*, 438 U.S. at 171; *United States v. Ketzeback*, 358 F.3d 987, 990 (8th Cir. 2004); *United States v. Colkley*, 899 F.2d 297, 300 (4th Cir. 1990); *United States v. Martin*, 615 F.2d 318, 328 (5th Cir. 1980).

hearing in this case would be academic because there is no question the FISA application [or applications] passes [or pass] muster." *Medunjanin*, 2012 WL 526428, at *9. Under these circumstances, the defendant's motion for disclosure of the FISA materials should be denied.

C. THE DEFENDANT'S MOTION FOR NOTICE AND DISCOVERY OF EXECUTIVE ORDER 12333 INFORMATION SHOULD BE DENIED

The defendant also seeks notice and discovery of any information collected in this case pursuant to E.O. 12333. (Doc. 61 at 1.) In support of his motion, the defendant argues that: (1) 18 U.S.C. § 3504 requires the Government to provide notice of any use of E.O. 12333 information; (2) the Fourth and Fifth Amendments of the U.S. Constitution, as well as the Federal Rules of Criminal Procedure (FRCP) 12(b)(3)(C) and 16 (a)(1)(E)(i), require the Government to provide notice of any use of E.O. 12333 information; and (3) use of E.O. 12333 information violates the Fourth Amendment of the Constitution. (Doc. 61 at 8-19.) The motion should be denied without a hearing.

[CLASSIFIED MATERIAL REDACTED].

Further, the government has complied with its notice and discovery obligations. These obligations are not limitless. *See United States v. Agurs*, 427 U.S. 97, 106 (1976) (noting that the government is under "no duty to provide defense counsel with unlimited discovery of everything known by the prosecutor"); *United States v. Phillips*, 854 F.2d 273, 277 (7th Cir. 1988) (finding that discovery rules do "not grant criminal defendants unfettered access to government files"); *United States v. Griebel,* 312 F. App'x 93, 96 (10th Cir. 2008) (the government's discovery obligations "are defined by Rule 16, *Brady*, *Giglio*, and the Jencks Act"); *United States v. Conyers*, No. 15-Cr-537(VEC), 2016 WL 7189850, at *7-11 (S.D.N.Y. Dec. 9, 2016) (addressing the government's discovery obligations). Further, there is no rule of discovery that requires the government to provide a defendant with a clear, concise narrative regarding the

origins of the criminal investigation that led to his arrest. *See Pennsylvania v. Ritchie*, 480 U.S. 39, 59 (1987) ("[D]efendant's right to discover exculpatory evidence does not include the unsupervised authority to search through the [government's] files"); *United States v. Bagley*, 473 U.S. 667, 675 (1985) ("[T]he prosecutor is not required to deliver his entire file to defense counsel"). Rather, the government is required to provide the defense with all discoverable material (including exculpatory information) described in FRCP 16.

Notice concerning the government's intent to use evidence in a criminal case is generally governed by FRCP 12 and 16. FRCP 12(b)(4)(B) provides in relevant part:

> [T]he defendant may, in order to have an opportunity to move to suppress evidence under Rule 12(b)(3)(C), request notice of the government's intent to use (in its evidence-in-chief at trial) any evidence that the defendant may be entitled to discover under Rule 16.

The purpose of this rule is to "provide the defendant with sufficient information to file the necessary suppression motions." *United States v. Ishak*, 277 F.R.D. 156, 158 (E.D. Va. 2011). "Thus, the government's obligation under Rule 12(b)(4)(B) ends when it has made disclosures that sufficiently allow the defendant to make informed decisions whether to file one or more motions to suppress." *Id.* The government has satisfied this obligation and provided the defendant with sufficient information and notice to file any necessary motions to suppress. No court has interpreted FRCP 12(b)(4)(B) to require the government to give an accounting of every investigative technique used in the case, regardless of its relationship to admissible evidence. Rather, in a criminal case, defense counsel analyzes the discovery, determines what suppression motions to make, and files them. The government then responds. That is precisely what has occurred in the instant case. For these reasons, the defendant's request for more information than any rule or statute requires should be denied.

The government's notice obligations regarding the use of FISA information under 50 U.S.C. §§ 1806(f) and 1825(d) apply only if the government (1) "intends to enter into evidence or otherwise use or disclose" (2) "against an aggrieved person" (3) in a "trial, hearing, or other proceeding in or before any court, department officer, agency, regulatory body, or other authority of the United States" (4) any "information obtained or derived from" (5) "electronic surveillance [or physical search] of that aggrieved person." 50 U.S.C. §§ 1806(f), 1825(d). Where all five criteria are met, the government will notify the defendant and the Court that the United States intends to use or disclose such information. The government has complied with those provisions in this case. On July 21, 2016, the government provided the defendant with notice pursuant to 50 U.S.C. §§ 1806(c) and 1825(d) that it intended to use evidence "obtained or derived from electronic surveillance and physical search" conducted pursuant to FISA against the defendant at trial. (Doc. 14). The government's notice gave the defendant all the information to which he was entitled and that was necessary to file a motion to suppress.

In the context of FISA collection, Congress has made a decision to allow for greater protection of information than is normally afforded because of the need to protect sensitive national security information, which includes classified sources and methods. Congress intended that FISA "reconcile national intelligence and counterintelligence needs with constitutional principles in a way that is consistent with both national security and individual rights." *See* S. Rep. No. 95-701, 95th Cong., 2d Sess., 39, at 16 (quoting *Keith*, 407 U.S. at 323) (1978). As such, in recognition of "the nature of the national interests implicated in matters involving a foreign power or its agents," Congress provided for more limited disclosure than is ordinarily provided with regard to criminal evidence. *Belfield*, 692 F.2d at 148.

The defendant's position that he is entitled to more information regarding FISA-authorized collection is further refuted by the fact that Congress did provide for broader notice of FISA surveillance in certain situations, but declined to do so in the notice sections applicable to criminal defendants. *See Dean v. United States*, 556 U.S. 568, 573 (2009) ("[W]here Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion."). Specifically, Congress identified three scenarios where more specific notice regarding FISA surveillance was warranted. *See* 50 U.S.C. § 1806(j) (notice of particular information regarding surveillance required where the Attorney General approves emergency surveillance and the government does not later obtain authorization from the FISC); 50 U.S.C. § 1825(b) (requiring notice identifying property seized, altered, or reproduced during physical search of a U.S. person's residence where the Attorney General has determined that there is no national security interest in continued secrecy); 50 U.S.C. § 1825(j) (notice of particular information regarding physical search required where the Attorney General approves emergency physical search and the government does not later obtain authorization from the FISC). Congress elected not to require such broad disclosure in the situation where a defendant is charged in a criminal proceeding. *See* 50 U.S.C. §§ 1806(c), 1825(d) (requiring only notice that "the United States intends" to use or disclose FISA-obtained or -derived information).

Nevertheless, the defendant argues that he is entitled to additional notice and discovery under 18 U.S.C. § 3504. (Doc. 61 at 8-11). That section provides in relevant part:

> In any trial, hearing, or other proceeding in or before any court . . . [u]pon a claim by a party aggrieved that evidence is inadmissible because it is the primary product of an unlawful act or because it was obtained by exploitation of an unlawful act, the opponent of

> the claim shall affirm or deny the occurrence of the alleged unlawful act.

However, 18 U.S.C. § 3504 is not applicable here because no "unlawful act" has occurred. 18 U.S.C. § 3504(a)(1) & (b). The FISA evidence was not the product of an unlawful act; to the contrary, it was lawfully obtained pursuant to orders of the FISC.[22] Moreover, the government provided the notice required under the FISA statute (50 U.S.C. §§ 1806(c) and 1825(d)), which is the more specific notice provision that applies in this case. No court has held that in addition to 50 U.S.C. §§ 1806(c) or 1825(d), the government has an additional notice requirement under 18 U.S.C. § 3504. A specific statutory provision normally controls over one of more general application. *Bloate v. United States*, 559 U.S. 196, 207 (2010); *Gozlon-Peretz v. United States*, 498 U.S. 395, 407 (1991). Moreover, 50 U.S.C. § 1806 was enacted in 1978 and 50 U.S. C. § 1825 was enacted in 1994, years after 18 U.S.C. § 3504 was adopted in 1970. *See* Organized Crime Control Act of 1970, Pub. L. No. 91-452, § 702, 84 Stat. 922, 935-36 (1970); and Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, § 807, 108 Stat. 3423, 3443 (1994). A later enacted statute may limit the scope of an earlier statute. *See Food and Drug Admin. v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 143 (2000); *Nutrition Health Alliance v. Food and Drug Administration*, 318 F.3d 92, 102 (2d Cir. 2003); *Bhd. of Maintenance of Way Emp. v. CSX Transp., Inc.*, 478 F.3d 814, 817 (7th Cir. 2007); *see also Acosta v. Gonzales*, 439 F.3d 550, 555 (9th Cir. 2006) ("[C]onflicting statutes should be interpreted so as to give effect to each but to allow a later enacted, more specific statute to amend an earlier, more general statute.") (citations omitted). Thus, there is no basis for holding that 18 U.S.C. § 3504 trumps FISA's later-enacted, more specific notice provisions.

---

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

Moreover, the defendant has failed to establish a colorable basis to believe that he has been aggrieved by unlawful surveillance of any kind. *See United States v. Pacella*, 622 F.2d 640, 643 (2d Cir. 1980) ("Although the claim need not be particularized, it may not be based upon mere suspicion but must at least appear to have a 'colorable' basis before it may function to trigger the government's obligation to respond under § 3504" (quoting *United States v. Yanagita*, 522 F.2d 770, 774 (2d Cir. 1976))); *In re Millow*, 529 F.2d 770, 774 (2d Cir. 1976) (where "assertions of misconduct are so obviously frivolous and lack even a colorable basis there is no 'claim'"). Although the defendant argues that a colorable basis exists because the Government referenced "§ 1813 in its FISA notice" and because he suspects "widespread collection and retention of American's information under E.O. 12333," his argument is seriously misplaced. (Doc. 61 at 9-10).

In its April 17, 2017, letter to this Court (Doc. 51), the Government explained that Section 1813 was referenced in the FISA Notice as part of a string citation to Subchapter I of the statute, which is codified at Sections 1801 through 1813 of Title 50. Thus, the Government simply intended to cite to, and provide notice of the use of, traditional Title I FISA authority; there is no other significance to the inclusion of Section 1813, and it was not intended to be a reference to E.O. 12333. Additionally, the defendant makes only bare assertions, together with citations to newspaper articles and editorials about such collection, which is exactly the type of showing that courts have found insufficient to establish a colorable claim of illegality. *See, e.g.*, *United States v. Aref*, 285 F. App'x 784, 793 (2d Cir. 2008) (summary order) (finding insufficient defendant's showing that consisted of statements "by unnamed sources in a newspaper article"); *United States v. Londono-Cardoña*, No. 05-Cr-10304 (GAO), 2008 WL 313473, at *2 (D. Mass. Feb. 1, 2008) (finding insufficient defendants' showing of proffered

Drug Enforcement Agency teletype messages that referred "only to apparently *lawful* surveillance in Colombia," and a newspaper article discussing alleged warrantless domestic wiretapping that had "no relevance" to the defendants' case); *In re Grand Jury Investigation*, 431 F. Supp. 2d 584, 591 (E.D. Va. 2006) (finding insufficient defense showing of "bare allegations that the government has been intercepting communications through illegal electronic surveillance").

Several courts nationwide have rejected similar motions under 18 U.S.C. § 3504 for notice and disclosure of surveillance in the context of FISA litigation. In *United States v. Aref*, 285 F. App'x 784, 793 (2d Cir. 2008) (summary order), the Second Circuit affirmed the district court's denial of defendant's Section 3504 motion for notice and disclosure of surveillance. In so ruling, the Second Circuit stated that the defendant's mere identification of representations from unnamed sources in a newspaper article, coupled with defendant's interpretation of the prosecutor's pattern of objections, was insufficient to form a colorable basis for a claim under Section 3504. *Id.*

Recently, in *United States v. El Gammal*, No. 15 Cr. 588 (E.R.) (S.D.N.Y.), Judge Edgardo Ramos denied a similar motion for an order compelling notice and discovery of searches, seizures, and surveillance techniques. (Doc. 150). Like the present motion, the motion in *El Gammal* was made under 18 U.S.C. § 3504, FRCP 12(b)(3)(c) and 16(a)(1)(E)(i), and the Fourth and Fifth Amendments and speculated based on a "suspicion" that the defendant was surveilled under E.O. 12333.

Recently, a district court in the Middle District of Pennsylvania ruled on the viability of a Section 3504 motion in the FISA suppression context. *United States v. Aziz*, No. 15-Cr-309, 2017 WL 118253, *5 (M.D. Pa. Jan. 12, 2017). In *Aziz*, the defendant was given proper statutory

notice of the Government's intent to use FISA information. The defendant then moved, in part under Section 3504, for notice and disclosure of surveillance authorities as well as suppression of the fruits of any other collection conducted under FISA or other "confidential" foreign intelligence gathering. *Id.* In denying the defendant's motion, the court held that "in cases involving FISA information, a suppression motion pursuant to §§ 1806(e) or 1825(f) is the procedure clearly contemplated by the foreign intelligence statutes for resolving allegations of unlawful surveillance." *Id.* (internal quotations and citation omitted). *Aziz* further held that "FISA's particularized notice, disclosure, and suppression procedures supplant the requirements of § 3504." *Id.*

Similarly, in *United States v. Thomas*, 201 F. Supp. 3d 643, 648 (E.D. Pa. 2016), the district court denied a defendant's speculative motion under Section 3504 for notice and discovery of surveillance techniques, noting that suppression motions under the FISA rubric are the "procedure clearly contemplated by the foreign intelligence statutes for resolving allegations of unlawful surveillance. *Id.* *Thomas* further held that a "suppression motion would solve a key problem with Defendant's current argument under 18 U.S.C. § 3504. As currently written, the pending Motion only speculates that Defendant could have been subject to illegal surveillance without directly accusing the Government of having done so. This is insufficient to trigger the Government's response requirement." *Id.* In sum, the defendant's frivolous speculation that there is widespread, unlawful E.O. 12333 collection and, thus, he is somehow affected contradicts the dictates of *Pacella* and *Millow*. For all of the foregoing reasons, the defendant's motion should fail.[23]

[23] **[CLASSIFIED MATERIAL REDACTED]**.

VI. CONCLUSION: THERE IS NO BASIS FOR THE COURT TO SUPPRESS THE FISA INFORMATION, DISCLOSE THE FISA MATERIALS, OR REQUIRE THE GOVERNMENT TO PROVIDE NOTICE AND DISCOVERY OF E.O. 12333 COLLECTION

For the foregoing reasons, the defendant's motions should be denied without a hearing. The Attorney General has filed a declaration in this case stating that disclosure of or an adversary hearing with respects to the FISA materials 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 information was lawfully acquired and whether the electronic surveillance and physical search were made in conformity with an order of authorization or approval. 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]." 50 U.S.C. §§ 1806(f), 1825(g). Congress, in enacting FISA's procedures for *in camera, ex parte* judicial review, has balanced and accommodated the competing interests of the Government and criminal defendants, and has articulated the standard for disclosure; that is, only where the Court finds that disclosure is necessary to the Court's accurate determination of the legality of the FISA collection.

The Government respectfully submits that the Court can make this determination without disclosing the classified and highly sensitive FISA materials to the defendant. The FISA materials at issue here, which have been submitted for *in camera, ex parte* review in the Sealed Appendix, are organized and readily understood, and an overview of them has been presented herein as a frame of reference. This Court will be able to render a determination based on its *in camera, ex parte* review, and the defendant has failed to present any colorable basis for supplanting Congress' reasoned judgment with a different proposed standard of review.

Furthermore, the Government respectfully submits that the Court's examination of the FISA materials in the Sealed Appendix will demonstrate that the Government satisfied FISA's requirements to obtain orders for electronic surveillance and physical search, that the information obtained pursuant to FISA was lawfully acquired, and that the electronic surveillance and physical search were made in conformity with an order of authorization or approval.

Even if this Court were to determine that the FISA information was not lawfully acquired or that the electronic surveillance and physical search were not made in conformity with an order of authorization or approval, 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 also Ning Wen*, 477 F.3d at 897 (stating that the *Leon* good-faith exception applies to FISA orders); *Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *25 n.8.

Based on the foregoing analysis, the Government respectfully submits that the Court must conduct an *in camera*, *ex parte* review of the FISA materials and the Government's classified submission, and should: (1) find that the electronic surveillance and physical search at issue in this case were both lawfully authorized and lawfully conducted; (2) hold that disclosure of the FISA materials and the Government's classified submissions to the defendant is not authorized because the Court is able to make an accurate determination of the legality of the surveillance and search without disclosing the FISA materials or any portions thereof; (3) hold that the fruits of electronic surveillance and physical search should not be suppressed; (4) deny the defendant's motions without an evidentiary hearing; and (5) order that the FISA materials and the Government's classified submissions be maintained under seal by the Classified Information Security Officer or his or her designee.[24]

[24] A district court order granting motions or requests under 50 U.S.C. §§ 1806(g) or 1825(h), a

Respectfully submitted,

JOON H. KIM
Acting United States Attorney

By: /s/ Emil J. Bove III
Emil J. Bove III
George D. Turner
Assistant U.S. Attorneys
(212) 637-2444

/s/ Joseph Attias
Joseph Attias
Trial Attorney
National Security Division
U.S. Department of Justice

/s/ Chad M. Davis
Chad M. Davis
Attorney Advisor
National Security Division
U.S. Department of Justice

Attorneys for United States of America

---

decision that electronic surveillance or physical search was not lawfully authorized or conducted, and an order requiring the disclosure of FISA materials is each a final order for purposes of appeal. 50 U.S.C. §§ 1806(h), 1825(i). Should the Court conclude that disclosure of any item within any of the FISA materials or suppression of any FISA-obtained or -derived information may be required, given the significant national security consequences that would result from such disclosure or suppression, 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, and that the Court stay any such order pending an appeal by the United States of that order.