```
1 EILEEN M. DECKER
   United States Attorney
 2 PATRICIA A. DONAHUE
   Assistant United States Attorney
   Chief, National Security Division
  JUDITH A. HEINZ (Cal. Bar No. 176264)
   Assistant United States Attorney
  Senior Litigation Counsel, National Security Division
        1500 United States Courthouse
        312 North Spring Street
        Los Angeles, California 90012
        Telephone: (213) 894-7280
 6
        Facsimile: (213) 894-7631
        E-mail:
                  judith.heinz@usdoj.gov
  DEIRDRE Z. ELIOT (Cal. Bar No. 145007)
   Assistant United States Attorney
  Terrorism and Export Crimes Section
        8000 United States Courthouse
        411 West Fourth Street
 9
        Santa Ana, California 92701
        Telephone: (714) 338-3599
10
        Facsimile: (714) 338-3564
        E-mail:
                deirdre.eliot@usdoj.gov
11
   Attorneys for Plaintiff
  UNITED STATES OF AMERICA
12
                       UNITED STATES DISTRICT COURT
13
                  FOR THE CENTRAL DISTRICT OF CALIFORNIA
14
                             SOUTHERN DIVISION
15
   UNITED STATES OF AMERICA,
                                      No. SA CR 15-00060(A)-DOC
16
           Plaintiff,
                                      GOVERNMENT'S UNCLASSIFIED
                                      MEMORANDUM IN OPPOSITION TO
17
                 v.
                                      DEFENDANTS' MOTIONS
18
  NADER SALEM ELHUZAYEL and
                                      Hearing Date: April 28, 2016
   MUHANAD ELFATIH M. A. BADAWI,
                                      Hearing Time: 12:00 noon
19
                                      Location:
                                                    Courtroom of the
           Defendants.
                                                    Hon. David O. Carter
20
21
        Plaintiff United States of America, by and through its counsel
22 of record, the United States Attorney for the Central District of
23||California and Assistant United States Attorneys Judith A. Heinz
   and Deirdre Z. Eliot, hereby files its UNCLASSIFIED MEMORANDUM IN
   OPPOSITION TO DEFENDANT ELHUZAYEL'S MOTION FOR DISCLOSURE OF FISA-
25
```

RELATED MATERIAL AND TO SUPPRESS THE FRUITS OR DERIVATIVES OF

ELECTRONIC SURVEILLANCE AND ANY OTHER MEANS OF COLLECTION CONDUCTED PURSUANT TO FISA OR OTHER FOREIGN INTELLIGENCE GATHERING AND 3 DEFENDANT BADAWI'S MOTION TO SUPPRESS EVIDENCE COLLECTED PURSUANT TO FISA WARRANT AND JOINDER IN CO-DEFENDANT'S MOTIONS. This UNCLASSIFIED MEMORANDUM is based upon the attached memorandum of points and authorities, a sealed appendix, and the files and records in this case. Dated: March 10, 2016 Respectfully submitted, 8 EILEEN M. DECKER United States Attorney 9 PATRICIA A. DONAHUE 10 Assistant United States Attorney Chief, National Security Division 11 12 /s/ JUDITH A. HEINZ DEIRDRE Z. ELIOT 13 Assistant United States Attorneys Central District of California 14 15 MICHAEL DITTOE Trial Attorney Counterterrorism Section 16 National Security Division United States Department of Justice 17 /s/ 18 PURVI PATEL Attorney Advisor 19 Office of Intelligence National Security Division United States Department of Justice 20 Attorneys for Plaintiff 21 UNITED STATES OF AMERICA 22 23l 24 25

1		TABLE OF CONTENTS
2	l.	INTRODUCTION1
	i	A. BACKGROUND3
3		B. OVERVIEW OF THE FISA AUTHORITIES6
		1. [CLASSIFIED MATERIAL REDACTED]6
4		2. [CLASSIFIED MATERIAL REDACTED]6
5		3. The FISC's Findings6
6	II.	THE FISA PROCESS6
7		A. OVERVIEW OF FISA6
		B. THE FISA APPLICATION8
8		1. The Certification11
		2. Minimization Procedures11
9		3. Attorney General's Approval
10	,	C. THE FISC'S ORDERS12
11	III.	THE DISTRICT COURT'S REVIEW OF FISC ORDERS
		A. THE REVIEW IS TO BE CONDUCTED IN CAMERA AND EX PARTE18
12	[1. In Camera, Ex Parte Review is the Rule20
13		2. In Camera, Ex Parte Review is Constitutional26
		B. THE DISTRICT COURT'S SUBSTANTIVE REVIEW28
14		1. Standard of Review of Probable Cause28
15		2. Probable Cause Standard30
		3. Standard of Review of Certifications
16		4. FISA is Subject to the "Good-Faith"
17		Exception35
18	IV.	THE FISA INFORMATION WAS LAWFULLY ACQUIRED AND THE ELECTRONIC
		SURVEILLANCE AND PHYSICAL SEARCHES WERE MADE IN CONFORMITY
19		WITH AN ORDER OF AUTHORITIZATION OR APPROVAL
		A. THE INSTANT FISA APPLICATIONS MET FISA'S PROBABLE
20		CAUSE STANDARD37
21		1. [CLASSIFIED MATERIAL REDACTED]
		2. [CLASSIFIED MATERIAL REDACTED]
22		a. [CLASSIFIED MATERIAL REDACTED]
23		i. [CLASSIFIED MATERIAL REDACTED]
.		ii. [CLASSIFIED MATERIAL REDACTED]
24		iii. [CLASSIFIED MATERIAL REDACTED]
25		v. [CLASSIFIED MATERIAL REDACTED]
- ~	1	V. [CHAPPIETED MATERIAN REDACTED]

1	b. [CLASSIFIED MATERIAL REDACTED]38
ĺ	i. [CLASSIFIED MATERIAL REDACTED]38
2	ii. [CLASSIFIED MATERIAL REDACTED]38
3	iii. [CLASSIFIED MATERIAL REDACTED]38
	iv. [CLASSIFIED MATERIAL REDACTED]39
4	v. [CLASSIFIED MATERIAL REDACTED]39
إ	3. The FISC Correctly Concluded that the Targeted
5	Facilities or Places Were Being Used, or Were About
6	to be Used, by the Targets of the Electronic
	Surveillance and that the Targeted Premises or
7	Property Were, or Were About to be Owned, Used, Possessed by or in Transit to or from, the Targets of
8	the Physical Searches
	a. [CLASSIFIED MATERIAL REDACTED]
9	i. [CLASSIFIED MATERIAL REDACTED]39
_	ii. [CLASSIFIED MATERIAL REDACTED]39
10	iii. [CLASSIFIED MATERIAL REDACTED]39
11	iv. [CLASSIFIED MATERIAL REDACTED]39
	v. [CLASSIFIED MATERIAL REDACTED]39
12	vi. [CLASSIFIED MATERIAL REDACTED]39
13	b. [CLASSIFIED MATERIAL REDACTED]39
	i. [CLASSIFIED MATERIAL REDACTED]39
14	ii. [CLASSIFIED MATERIAL REDACTED]40
_	iii. [CLASSIFIED MATERIAL REDACTED]40
15	iv. [CLASSIFIED MATERIAL REDACTED]40
16	c. Conclusion: There Was Sufficient Probable Cause
	to Establish that the Information Acquired from
17	the Targeted Facilities, Places, Property,
18	or Premises Was Lawfully Acquired40
10	B. THE CERTIFICATIONS COMPLIED WITH FISA40
19	1. Foreign Intelligence Information40
	2. "A Significant Purpose"40
20	3. Information Not Reasonably Obtainable
21	Through Normal Investigative Techniques40
22	C. ELECTRONIC SURVEILLANCE AND PHYSICAL SEARCHES WERE
23	CONDUCTED IN COMFORMITY WITH AN ORDER OF AUTHORIZATION
∠ ع	OR APPROVAL
24	1. The Standard Minimization Procedures41
	2. The FISA Information Was Appropriately Minimized47
25	

Case 8:15-cr-00060-DOC Document 88 Filed 03/14/16 Page 5 of 79 Page ID #:342

l	
1	V. THE COURT SHOULD REJECT THE DEFENDANTS' LEGAL ARGUMENTS47
2	A. THE DEFENDANTS HAVE NOT ESTABLISHED ANY BASIS FOR THE
	COURT TO SUPPRESS THE FISA INFORMATION48 1. The Government Satisfied the Probable Cause
3	Requirements of FISA
4	2. Franks v. Delaware Does Not Require
5	Suppression of FISA Materials50
اے	3. The Certifications Complied with FISA54 4. The Government Complied with the Minimization
6	Procedures55
7	B. THE DEFENDANTS HAVE NOT ESTABLISHED ANY BASIS FOR
8	THE COURT TO DISCLOSE FISA MATERIALS
9	1. Disclosure is Not "Necessary" under FISA56 2. Due Process Does Not Require Disclosure60
	3. The Adversary System Does Not Require Disclosure61
10	
11	VI. CONCLUSION: THERE IS NO BASIS TO DISCLOSE THE FISA MATERIALS OR TO SUPPRESS THE FISA INFORMATION
12	THIRD ON TO BOTTALDS THE TIDA INFORMATION
1 2	
13	
14	
15	
16	
1 17	
17	
18	
19	
20	
21	
22	
23	
24	
25	

TABLE OF AUTHORITIES FEDERAL CASES ACLU Found. of So. Cal. v. Barr. 3 Baldrawdi v. Dep't of Homeland Sec., 596 F. Supp. 2d 389 (D. Conn 2009)......56 Barhoumi v. Obama, 6 609 F.3d 416 (D.C. Cir. 2010)......49 CIA v. Sims, 8 Draper v. United States, 358 U.S. 307 (1959)......50 10 Franks v. Delaware, 11 Halperin v. CIA, 12 629 F.2d 144 (D.C. Cir. 1980)......25 13 Illinois v. Gates, 14 In re Grand Jury Proceedings of the Spec. Apr. 2002 Grand Jury, 15 16 In re Kevork, 634 F. Supp. 1002 (C.D. Cal. 1985), aff'd, 17 18 In re Sealed Case, 19 Latif v. Obama, 20 666 F.3d 746 (D.C. Cir. 2011)......49 21 Los Angeles County v. Davis, 440 U.S. 625 (1979)......54 22 Massachusetts v. Sheppard, 23 $24 \parallel$ Mayfield v. United States, 504 F. Supp. 2d 1023 (D. Or 2007) 25 588 F.3d 1252 (9th Cir. 2009)......54

1	
	Phillippi v. CIA, 655 F.2d 1325 (D.C. Cir. 1981)
3	Scott v. United States, 436 U.S. 128 (1978)45
4	
5	United States v. Abu-Jihaad, 531 F. Supp. 2d 299 (D. Conn. 2008), aff'd, 630 F.3d 102 (2d Cir. 2010)passim
6	
7	United States v. Ahmed, No. 1:06-CR-147, 2009 U.S. Dist. Lexis 120007 (N.D. Ga. Mar. 19, 2009)
8	United States v. Alwan,
9	
10 11	United States v. Amawi, 2009 WL 961143 (N.D. Ohio Apr. 7 2009)57
ľ	United States v. Badia, 827 F.2d 1458 (11th Cir. 1987)22, 33, 34, 35, 59
13	United States v. Belfield, 692 F.2d 141 (D.C. Cir. 1982)20, 23, 25, 27, 53, 58, 60, 63
15	United States v. Benkahla,
16	437 F. Supp. 2d 541 (E.D. Va. 2006)
	United States v. Bin Laden, 126 F. Supp. 2d 264 (S.D.N.Y. 2000)
18 19	United States v. Bynum, 485 F.2d 490 (2d Cir. 1973)44
20	United States v. Campa, 529 F.3d 980 (11th Cir. 2008)
21	United States v. Canfield, 212 F.3d 713 (2d Cir. 2000)
22	
23	United States v. Cavanagh, 807 F.2d 787 (9th Cir. 1987)
24	United States v. Colkley, 899 F.2d 297 (4th Cir. 1990)51, 52

```
1 United States v. Damrah,
   United States v. Daoud,
   2014 WL 321384 (N.D. Ill. Jan. 29, 2014), rev'd
3
   United States v. Duggan,
   6 United States v. Duka,
   671 F.3d 329 (3d Cir. 2011)......18, 30, 36
 United States v. El-Mezain,
81
   664 F.3d 467
   United States v. Falcone,
   364 F. Supp. 877 (D.N.J. 1973), aff'd,
   11
 United States v. Falvey,
   12
13 United States v. Garcia,
   14
 United States v. Gowadia.
   No. 05-00486, 2009 WL 1649714
15
   16l
 United States v. Hammoud,
   381 F.3d 316 (4th Cir. 2004), rev'd on other grounds,
17
   543 U.S. 1097 (2005), op. reinstated in pertinent part,
   18
 United States v. Hassan,
19||
   742 F.3d 104 (4th Cir. 2014)......57
20
 United States v. Hassoun,
   21
 United States v. Hussein,
  2014 WL 1682845 (S.D. Cal. April 29, 2014)......62
23
 United States v. Isa,
   923 F.2d 1300 (8th Cir. 1991)......20, 21, 26, 46, 62, 63
24
```

	United States v. Islamic Am. Relief Agency, No. 07-00087-CR-W-NKL, 2009 WL 5169536
2	(W.D. Mo. Dec. 21, 2009)
3	United States v. Jamal, 2011 U.S. Dist. LEXIS 12224 (D. Az. February 11, 2011)62
5	United States v. Jayyousi, No. 04-60001, 2007 WL 851278 (S.D. Fla. Mar. 15, 2007), aff'd, 657 F.3d 1085 (11th Cir. 2011)
6 7	United States v. Joseph, 709 F.3d 1082 (11th Cir. 2013)29
8 9	United States v. Kashmiri, No. 09-CR-830, 2010 WL 4705159 (N.D. Ill. Nov. 10, 2010)
10	United States v. Ketzeback, 358 F.3d 987 (8th Cir. 2004)
11	United States v. Krupa,
Į	United States v. Lahiji, 2013 WL 550492 (D. Or. February 12, 2013)
14	United States v. Leon, 468 U.S. 897 (1984)
16 17	United States v. Martin, 615 F.2d 318 (5th Cir. 1980)52
	United States v. Martinez-Garcia, 397 F.3d 1205 (9th Cir. 2005)50
Ì	United States v. Marzook, 435 F. Supp. 2d 778 (N.D. Ill. 2006)
20	United States v. Medunjanin, No. 10-CR-19-1, 2012 WL 526428
22	(S.D.N.Y. Feb. 16, 2012)47, 59
23	United States v. Megahey, 553 F. Supp. 1180 (E.D.N.Y. 1982)
24 25	United States v. Mohamud, 2014 WL 2866749 (D. Or., June 24, 2014)

Case 8:15-cr-00060-DOC Document 88 Filed 03/14/16 Page 10 of 79 Page ID #:347

(ase 8:15-cr-00060-DOC Document 88 Filed 03/14/16 Page 11 of 79 Page ID #:348
	United States v. Smith, 581 F.3d 692 (8th Cir. 2009)29
3	United States v. Spanjol, 720 F. Supp. 55 (E.D. Pa. 1989), aff'd,
4	958 F.2d 365 (3d Cir. 1992)
5	United States v. Stewart, 590 F.3d 93 (2d Cir. 2009)22
	United States v. Thomson, 752 F. Supp. 75 (W.D.N.Y. 1990)
7	United States v. United States District Court, 407 U.S. 297 (1972)
	United States v. U.S. Gypsum Co., 333 U.S. 364 (1948)35
	United States v. Warsame, 547 F. Supp. 2d 982 (D. Minn. 2008)
12	United States v. Yunis, 867 F.2d 617 (D.C. Cir. 1989)25
14	U.S. CONSTITUTION
15	Amend. I
16	Amend. IV
17	Amend. V
18 19	Amend. VI
20	FEDERAL STATUTES
21	50 U.S.C. § 1801
22	50 U.S.C. §§ 1801-1812
23	50 U.S.C. § 1803
24	50 U.S.C. § 1804
25	50 U.S.C. § 1805

Case 8:15-cr-00060-DOC Document 88 Filed 03/14/16 Page 12 of 79 Page ID #:349

1|| I. INTRODUCTION

16

22

23

24

The Government is filing this unclassified memorandum in 3 opposition to defendant Nader Salem Elhuzayel's ("Elhuzayel") 4 Motion for Disclosure of [the Foreign Intelligence Surveillance 5||Act ("FISA")]-Related Material and to Suppress the Fruits or 6 Derivatives of Electronic Surveillance and Any Other Means of 7 Collection Conducted Pursuant to FISA or Other Foreign Intelligence 8 Gathering" (Docket Entry ("Doc.") 69) and defendant Muhanad Elfatih 9||M.A. Badawi's ("Badawi") "Motion to Suppress Evidence Collected 10 Pursuant to FISA Warrant; Joinder in Co-Defendant's Motions" (Doc. 11 70) (hereinafter, collectively referred to as "defendants' 12 motions"). The defendants' motions seek: (1) suppression of all 13 evidence obtained under FISA (i.e., "the FISA information"); and 14 (2) disclosure of the FISA applications, orders, and related 15 materials (i.e., "the FISA materials").1

The defendants' motions have triggered this Court's review of 17 the materials related to the FISA-authorized electronic 18 surveillance and physical searches to determine whether the FISA 19 information was lawfully acquired and whether the electronic 20 surveillance and physical searches were made in conformity with an 21 order of authorization or approval. Whenever "a motion is made"

¹ [CLASSIFIED MATERIAL REDACTED]

² [CLASSIFIED MATERIAL REDACTED]

³ The provisions of FISA that address the electronic surveillance at issue in this case are found at 50 U.S.C. §§ 1801-1812; those that 25 address physical searches are found at 50 U.S.C. §§ 1821-1829. These two

| pursuant to subsection (e)... to discover or obtain applications or 2 orders or other materials relating to electronic surveillance or to 3 discover, obtain or suppress evidence or information obtained or 4 derived from electronic surveillance under this Act, the United 5||States district court...shall...if the Attorney General files an 6 affidavit under oath that disclosure or an adversary hearing would 7 harm the national security of the United States, review in camera 8 and ex parte the application, order, and such other materials 9 relating to the surveillance as may be necessary to determine 10 whether the surveillance of the aggrieved person was lawfully 11 authorized and conducted." 50 U.S.C. §§ 1806(f), 1825(g). The 12 Government is filing herewith such an affidavit in which the 13 Attorney General claims under oath that disclosure or an adversary 14 hearing would harm the national security of the United States, 15 which is the prerequisite for the Court to review the FISA 16 materials in camera and ex parte; 4 consequently, the Government 17 respectfully submits that, for the reasons set forth hereinafter, 18||this Court must conduct an in camera, ex parte review of the

²⁰

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.

²⁴

⁴ The Attorney General's affidavit ("Declaration and Claim of Privilege") is filed both publicly and attached as part of the Government's classified filing. See Sealed Exhibit 1.

1 documents relevant to the defendants' motions in accordance with the provisions of 50 U.S.C. §§ 1806(f) and 1825(g).5

For the reasons set forth below and from the Court's in camera, ex parte review of the FISA materials, it is conclusively established that: (1) the electronic surveillance and physical 6 searches at issue in this case were both lawfully authorized and 7 | lawfully conducted in compliance with FISA; (2) disclosure to the 8 defendants of the FISA materials and the Government's classified 9 submissions is not authorized because the Court can make an 10 accurate determination of the legality of the FISA-authorized 11 electronic surveillance and physical searches without disclosing 12 the FISA materials or portions thereof; (3) the FISA materials 13 should not be disclosed; (4) the FISA information should not be 14 suppressed; and (5) no hearing is required.

A. BACKGROUND

2

3

15

16

24

25

On May 21, 2015, Elhuzayel and Badawi were arrested upon 17 complaint for conspiring to provide material support to the Islamic 18 State of Iraq and the Levant ("ISIL"), in violation of 18 U.S.C. 19 § 2339B. (Doc. 1) On June 3, 2015, Elhuzayel and Badawi were 20 indicted in the Central District of California ("CDCA") for 21 conspiring to provide material support to ISIL, in violation of 18 22 U.S.C. § 2339B. Elhuzayel was additionally charged with attempting 23||to provide material support to ISIL, in violation of 18 U.S.C.

⁵ [CLASSIFIED MATERIAL REDACTED]

1 2339B; and Badawi was additionally charged with aiding and 2 abetting an attempt to provide material support to ISIL, in violation of 18 U.S.C. §§ 2339B and 2. (Doc. 17) On October 7, 4 2015, a grand jury in the CDCA returned a superseding indictment 5 charging Elhuzayel and Badawi with conspiring to provide material 6 support to a foreign terrorist organization, in violation of 18 7 U.S.C. § 2339B. Elhuzayel was additionally charged with attempting 8 to provide material support to a foreign terrorist organization, in 9 violation of 18 U.S.C. § 2339B; and bank fraud, in violation of 18 10 U.S.C. §§ 1344 and 2. Badawi was additionally charged with aiding 11 and abetting an attempt to provide material support to a foreign 12 terrorist organization, in violation of 18 U.S.C. §§ 2339B and 2; and financial aid fraud, in violation of 18 U.S.C. § 1097(a). 14 (Doc. 41)

[CLASSIFIED MATERIAL REDACTED]

15

16

25

On June 8, 2015, pursuant to 50 U.S.C. § 1806(c), the United 17 States provided notice to both Elhuzayel and Badawi that it 18 "intends to offer into evidence, or otherwise use or disclose in 19 any proceedings in [this case], information obtained or derived 20 from electronic surveillance conducted pursuant to the Foreign 21 Intelligence Surveillance Act of 1978 (FISA), as amended, 50 U.S.C. 22 SS 1801-1812." (Doc. 23) On September 29, 2015, pursuant to 50 23||U.S.C. §§ 1806(c) and 1825(d), the United States provided an 24 updated notice to both Elhuzayel and Badawi stating that it

"intends to offer into evidence, or otherwise use or disclose in 2 any proceedings in [this case], information obtained or derived from electronic surveillance and physical searches conducted 4 pursuant to the Foreign Intelligence Surveillance Act of 1978 5||(FISA), as amended, 50 U.S.C. §§ 1801-1812 and §§ 1821-1829." 6 (Doc. 38) On January 29, 2016, the defendants filed their motions. (Doc. 69 and 70)

[CLASSIFIED MATERIAL REDACTED] 6

8

9

23

25

In subsequent sections of this Memorandum, the Government 10 will: (1) present an overview of the FISA authorities at issue in 11 this case; (2) discuss the FISA process; (3) address the manner in 12|| which the Court should conduct its in camera, ex parte review of 13 the FISA materials; (4) summarize the facts supporting the FISC's 14 probable cause determinations at issue (all of which information is 15 contained fully in the exhibits in the Sealed Appendix); (5) 16 discuss the relevant minimization procedures; and (6) address the 17 defendants' arguments in support of their motions. All of the 18 Government's pleadings and supporting FISA materials are being 19 submitted not only to oppose the defendants' requests, but also to 20 support the United States' request, pursuant to FISA, that this 21 Court: (1) conduct the required in camera, ex parte review of the 22 FISA materials; (2) find that the FISA information at issue was

⁶ As a result of the redactions, the pagination and footnote numbering of the classified memorandum and the unclassified memorandum are different.

lawfully acquired and that the electronic surveillance and physical 2||searches were conducted in conformity with an order of 3 authorization or approval; (3) find that the FISA information should be not be suppressed; and (4) order that none of the FISA 5 materials be disclosed to the defense, and instead, that they be 6 maintained by the United States under seal.

OVERVIEW OF THE FISA AUTHORITIES в.

[CLASSIFIED MATERIAL REDACTED]

- [CLASSIFIED MATERIAL REDACTED]
- [CLASSIFIED MATERIAL REDACTED]
 - [CLASSIFIED MATERIAL REDACTED]
- [CLASSIFIED MATERIAL REDACTED]
 - 3. The FISC's Findings
- [CLASSIFIED MATERIAL REDACTED]

15||II. THE FISA PROCESS

7

8

9

10

11

12

13

14

16

17

24

OVERVIEW OF FISA7

Enacted in 1978, and subsequently amended, FISA authorizes the 18 Chief Justice of the United States to designate eleven United 19 States District Judges to sit as judges of the FISC. 50 U.S.C. 20 | S 1803(a)(1). The FISC judges are empowered to consider ex parte 21 applications submitted by the Executive Branch for electronic 22 surveillance and physical searches when a significant purpose of 23 the application is to obtain foreign intelligence information, as

⁷ This memorandum references the statutory language in effect at the time relevant to this matter.

1 defined in FISA. Rulings of the FISC are subject to review by the 2||Foreign Intelligence Surveillance Court of Review ("FISC of 3 Review"), which is composed of three United States District or 4 Circuit Judges who are designated by the Chief Justice. 50 U.S.C. 5 § 1803(b).

As originally enacted, FISA required that a high-ranking 7 member of the Executive Branch of Government certify that "the 8 purpose" of the FISA application was to obtain foreign intelligence In 2001, FISA was amended as part of the Uniting and 9 information. 10 Strengthening America by Providing Appropriate Tools Required to 11 Intercept and Obstruct Terrorism Act ("USA PATRIOT Act").8 One 12 change to FISA accomplished by the USA PATRIOT Act is that a high-13 ranking official is now required to certify that the acquisition of 14 foreign intelligence information is "a significant purpose" of the 15 requested surveillance. 50 U.S.C. § 1804(a)(6)(B).

FISA provides that the Attorney General may authorize the 17 emergency employment of electronic surveillance and physical 18 searches 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 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;

16

19

20

21

22

23

24

⁸ Pub. L. No. 107-56, 115 Stat. 272 (2001).

- (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].

50 U.S.C. §§ 1805(e)(1), 1824(e)(1). Emergency electronic surveillance or physical searches must comport with FISA's minimization requirements, which are discussed below. See 50 U.S.C. §§ 1805(e)(2), 1824(e)(2). 10

THE FISA APPLICATION в.

1

2

3

4

5

10

11

13

14

15

16l

25

FISA provides a statutory procedure whereby the Executive Branch may obtain a judicial order authorizing the use of electronic surveillance, physical searches, or both, within the

9 [CLASSIFIED MATERIAL REDACTED]

¹⁰ If no FISC order authorizing the electronic surveillance or physical searches is issued, emergency surveillance or searches must 17 \parallel terminate when the information sought is obtained, when the FISC denies an application for an order, or after the expiration of seven days from 18 the time of the emergency employment, whichever is earliest. See 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 shall cause to be served on any U.S. person named in the application, and others in the FISC's discretion, 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. See 50 U.S.C. § 1806(j); see also 50 U.S.C. § 1824(j)(1) 21 (physical searches). In addition, if no FISC order is issued, neither information obtained nor evidence derived from the emergency electronic 22 surveillance or physical search may be disclosed in any court or other proceeding, and no information concerning a United States person acquired 23 from the electronic surveillance or physical search may be used in any other manner by Federal officers or employees without the person's consent, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm. See 50 U.S.C. §§ 1805(e)(5), 1824(e)(5).

United States where a significant purpose is the collection of foreign intelligence information. 11 50 U.S.C. §§ 1804(a)(6)(B), 1823(a)(6)(B). Under FISA, "[f]oreign intelligence information" means:

5

6

7

8

9

10

11

12

13

14

15

16

17

22

23

24

25

- (1) information that relates to, and if concerning a United States person¹² 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;
 - (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 searches may be conducted.

^{11 [}CLASSIFIED MATERIAL REDACTED]

^{12 [}CLASSIFIED MATERIAL REDACTED]

An application to conduct electronic surveillance pursuant to 2 FISA must contain, among other things:

> (1) the identity of the federal officer making the application;

1

311

4

5

6

7

8

9

10

11

12

13

14

15

16

17¹

18

19

21

- (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. 20 50 U.S.C. §§ 1804(a)(1)-(9).

An application to conduct a physical search pursuant to FISA 22 must contain similar information as an application to conduct 23 electronic surveillance except that an application to conduct a 24 physical search must also contain a statement of the facts and 25 circumstances that justify an applicant's belief that "the premises 1 or property to be searched contains foreign intelligence 2 information" and that each "premises or property to be searched is 3 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. The Certification

5

6

9

10

11

12

13

14

15

16

17

18

19

21

22

An application to the FISC for a FISA order must include a certification from a high-ranking executive branch official with 8 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).

Minimization Procedures

The Attorney General has adopted, and the FISC has approved, 23 minimization procedures that regulate the acquisition, retention, 24 and dissemination of non-publicly available information concerning unconsenting United States persons obtained through FISA-authorized 1 electronic surveillance or physical searches, including persons who 2 are not the targets of the FISA authorities. FISA requires that 3 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), 1821(4)(A).

4

5

6

14

15

16

19

20

24

25

In addition, minimization procedures also include "procedures 10 that allow for the retention and dissemination of information that 11 is evidence of a crime which has been, is being, or is about to be 12 committed and that is to be retained or disseminated for law 13 enforcement purposes." 50 U.S.C. §§ 1801(h)(3), 1821(4)(c).

[CLASSIFIED MATERIAL REDACTED]

Attorney General's Approval

FISA further requires that the Attorney General approve 17 applications for electronic surveillance, physical searches, or 18 both, before they are presented to the FISC.

THE FISC'S ORDERS C.

Once approved by the Attorney General, the application is 21 submitted to the FISC and assigned to one of its judges. The FISC 22||may approve the requested electronic surveillance, physical 23 searches, or both, 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 1 target of the electronic surveillance and/or physical search is a foreign power or an agent of a foreign power, 2 and that (B) the facilities or places at which the electronic surveillance is directed are being used, or 3 are about to be used, by a foreign power or an agent of a foreign power (or that the premises or property to be 4 searched is, or is about to be, owned, used, possessed by, or is in transit to or from, a foreign power or an 5 agent of a foreign power); 6 (3) the proposed minimization procedures meet the 7 statutory requirements set forth in 50 U.S.C. § 1801(h) (electronic surveillance) and 50 U.S.C. § 1821(4) 8 (physical search); 9 (4) the application contains all of the statements and certifications required by Section 1804 or Section 1823; 10 and 11 (5) if the target is a United States person, that the certifications are not clearly erroneous. 12 50 U.S.C. §§ 1805(a)(1)-(4), 1824(a)(1)-(4). 13 FISA defines "foreign power" to mean -14 (1) a foreign government or any component, thereof, 15 whether or not recognized by the United States; 16 (2) a faction of a foreign nation or nations, not substantially composed of United States persons; 17
 - (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;

18

19

20

21

22

23

24

- (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 is 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 therefore [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;

2

3

4

5

6

7

8

9

10

11

12

15

25

- (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 [the subparagraphs above] . . . or knowingly conspires with any person to engage in activities described in [the subparagraphs above.]

13||50 U.S.C. §§ 1801(b)(1) and (2); see also 50 U.S.C. § 1821(1) 14 (adopting definitions from 50 U.S.C. § 1801).

FISA specifies that no United States person may be considered 16 a foreign power or an agent of a foreign power solely on the basis 17 of activities protected by the First Amendment to the Constitution 18 of the United States. 50 U.S.C. §§ 1805(a)(2)(A), 1824(a)(2)(A). 19 Although protected First Amendment activities cannot form the sole 20 basis for FISA-authorized electronic surveillance or physical 21 searches, they may be considered by the FISC if there is other 22 activity indicative that the target is an agent of a foreign power. 23|| United States v. Rosen, 447 F. Supp. 2d 538, 549-50 (E.D. Va. 24 2006); United States v. Rahman, 861 F. Supp. 247, 252 (S.D.N.Y.

1 1994), aff'd, 189 F.3d 88 (2d Cir. 1999). Additionally, FISA
2 provides that "[i]n determining whether or not probable cause
3 exists . . . a judge may consider past activities of the target, as
4 well as facts and circumstances relating to current or future
5 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 searches, 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;

12

13

14

15

16

17

18

19

20

21

22

23

24

- (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) and 2(A); 1824(c)(1) and 2(A).

Under FISA, electronic surveillance or physical searches targeting a United States person may be approved for up to ninety 3 days, and those targeting a non-United States person may be approved for up to one-hundred and twenty days. 50 U.S.C. $5 | \S \S 1805(d)(1), 1824(d)(1).^{13}$ Extensions may be granted, but only if 6 the United States submits another application that complies with 7 FISA's requirements. An extension for electronic surveillance or 8||physical searches targeting a United States person may be approved g|| for up to ninety days, and one targeting a non-United States person 10 may be approved for up to one year. 14 50 U.S.C. §§ 1805(d)(2), 11 1824 (d) (2).

12 III. THE DISTRICT COURT'S REVIEW OF FISC ORDERS

13

21

22

25

FISA authorizes the use in a criminal prosecution of 14 information obtained or derived from any FISA-authorized electronic 15||surveillance or physical search, provided that advance 16 authorization is obtained from the Attorney General, 50 U.S.C. 17|| §§ 1806(b), 1825(c), and that proper notice is subsequently given 18 to the court and to each aggrieved person against whom the 19 information is to be used. 15 50 U.S.C. §§ 1806(c)-(d), 1825(d)-(e). 20 Upon receiving notice, an aggrieved person against whom the

^{13 [}CLASSIFIED MATERIAL REDACTED]

¹⁴ The FISC retains the authority to review, before the end of the 23 authorized period of electronic surveillance or physical searches, the Government's compliance with the requisite minimization procedures. 50 $24 \parallel U.S.C.$ §§ 1805(d)(3), 1824(d)(3).

^{15 [}CLASSIFIED MATERIAL REDACTED]

1 information is to be used may move to suppress the use of the FISA 2 information on two grounds: (1) that the information was unlawfully 3 acquired; or (2) that the electronic surveillance or physical 4 search was not conducted in conformity with an order of 5 authorization or approval. 50 U.S.C. §§ 1806(e), 1825(f). 6 addition, FISA contemplates that a defendant may file a motion or 7 request under any other statute or rule of the United States to g discover or obtain applications, orders, or other materials p relating to electronic surveillance or physical searches, i.e., the 10 FISA materials, 50 U.S.C. §§ 1806(f), 1825(g). When a defendant 11 moves to suppress FISA information under 50 U.S.C. §§ 1806(e) or 12 1825(f), or seeks to discover the FISA materials under some other 13 statute or rule, the motion or request is evaluated using FISA's 14 probable cause standard, which is discussed below, and not the 15 probable cause standard applicable to criminal warrants. See, 16 e.g., United States v. El-Mezain, 664 F.3d 467, 564 (5th Cir. ||17|||2011); United States v. Duka, 671 F.3d 329, 336-37 (3d Cir. 2011) 18 (rejecting appellant's challenge to FISA's probable cause standard 19 because it does not require any indication that a crime has been 20 committed); United States v. Pelton, 835 F.2d 1067, 1075 (4th Cir. 21 1987).

THE REVIEW IS TO BE CONDUCTED IN CAMERA AND EX PARTE

In assessing the legality of FISA-authorized electronic 24||surveillance and physical searches, or both, the district court

22

23

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 as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. ¹⁶

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]."¹⁷ 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 United States v. Nicholson, No. 09-CR-40, 2010 WL 1641167, at *4 (D. Or.

^{16 [}CLASSIFIED MATERIAL REDACTED]

¹⁷ In *United States v. Ott*, 827 F.2d 473, 476 (9th Cir. 1987), the Ninth Circuit "agree[d] with the district court that there [were] 'no indications of possible misrepresentation of fact, vague identification of the persons to be surveilled, or surveillance records which include a significant amount of non-foreign intelligence information, or any other factors that would indicate a need for disclosure' in the case."

1 Apr. 21, 2010) ("After an in-camera review, the court 'has the 2 discretion to disclose portions of the documents, under appropriate 3 protective procedures, only if [the court] decides that such 4 disclosure is necessary to make an accurate determination of the 5 legality of the surveillance.'") (quoting United States v. Duggan, 6 743 F.2d 59, 78 (2d Cir. 1984)) (emphasis in Nicholson); United 7 States v. Omar, No. 13-2195, slip op. at 10-11 (2015 WL 3393825, at 8 *5-6) (8th Cir. May 27, 2015) (citing *United States v. Isa*, 923 9|| F.2d 1300, 1306 (8th Cir. 1991)); United States v. Islamic Am. 10 Relief Agency ("IARA"), No. 07-00087-CR-W-NKL, 2009 WL 5169536, at 11 *3-4 (W.D. Mo. Dec. 21, 2009) ("FISA provides that Courts must 12 first review the challenged dockets ex parte and in camera"); E1-13 Mezain, 664 F.3d at 565; United States v. Abu-Jihaad, 630 F.3d 102, 14||129 (2d Cir. 2010); United States v. Belfield, 692 F.2d 141, 147 15|| (D.C. Cir. 1982); United States v. Kashmiri, No. 09-CR-830, 2010 WL 16||4705159, at *2 (N.D. Ill. Nov. 10, 2010).

In Camera, Ex Parte Review is the Rule

17

18

25

Federal courts, including the Ninth Circuit, have repeatedly 19 and consistently held that FISA anticipates that an ex parte, in 20 camera determination is to be the rule, while "[d]isclosure and an 21 adversary hearing are the exception, occurring only when 22 necessary." United States v. Sarkissian, 841 F.2d 959, 964 (9th 23||Cir. 1989) (quoting Belfield, 692 F.2d at 147); accord Omar, slip $24\|\text{op.}$ at 10 (2015 WL 3393825 at *5) (quoting *Isa*, 923 F.2d at 1306)

1 (emphasis in original); Nicholson, 2010 WL 1641167 at *3-4; El-2 Mezain, 664 F.3d at 567 ("[D]isclosure of FISA materials is the 3 exception and ex parte, in camera determination is the rule") $4\parallel$ (citing Abu Jihaad, 630 F.3d at 129); Duggan, 743 F.2d at 78; 5 Rosen, 447 F. Supp. 2d at 546; United States v. Spanjol, 720 F. 6 Supp. 55, 59 (E.D. Pa. 1989), aff'd, 958 F.2d 365 (3d Cir. 1992).

7

21

In fact, every court but one (whose decision was subsequently 8 overturned by an appellate court) 18 that has addressed a motion to gldisclose FISA materials or to suppress FISA information has been 10 able to reach a conclusion as to the legality of the FISA 11 collection at issue based on its in camera, ex parte review. See, ||e.g.|, Omar, slip op. at 10-11 (2015 WL 3393825 at *5-6); Isa, 923 13 F.2d at 1306 ("study of the materials leaves no doubt that |14| substantial national security interests required the in camera, ex 15 parte review, and that the district court properly conducted such a 16 review"); El-Mezain, 664 F.3d at 566 (quoting district court's 17 statement that no court has ever held an adversarial hearing to 18 assist the court); In re Grand Jury Proceedings of the Special Apr. 19|| 2002 Grand Jury ("In re Grand Jury Proceedings"), 347 F.3d 197, 203 20||(7th Cir. 2003) (noting that no court has ever ordered disclosure

¹⁸ The district court in *United States v. Daoud*, No. 12-CR-723 (N.D. Ill. Jan. 29, 2014), ruled that it was capable of making the determination, but nevertheless ordered the disclosure of FISA materials. The Government appealed the Daoud court's order to the U.S. Court of 23 Appeals for the Seventh Circuit, which overturned the district court's decision to disclose, stating, "So clear is it that the materials were 24 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 25||would have to do so." Daoud, 755 F.3d 479, 485 (7th Cir. 2014).

1 of FISA materials); United States. v. Stewart, 590 F.3d 93 (2d Cir. 2 2009); United States v. Abu-Jihaad, 531 F. Supp. 2d 299, 310 (D. 3 Conn. 2008), aff'd, 630 F.3d 102, 129-30 (2d Cir. 2010); United 4 States v. Jayyousi, No. 04-60001, 2007 WL 851278, at *7-8 (S.D. 5|| Fla. Mar. 15, 2007), aff'd, 657 F.3d 1085 (11th Cir. 2011); 19 United 6 States v. Badia, 827 F.2d 1458, 1463 (11th Cir. 1987); United $7 \parallel States \ v. \ Gowadia, \ No. \ 05-00486, \ 2009 \ WL \ 1649714, \ at *2 (D. Hawaii$ 8 June 8, 2009); Spanjol, 720 F. Supp. at 58-59; United States v. 9|| Sattar, No. 02-CR-395, 2003 WL 22137012, at *6 (S.D.N.Y. 2003) 10 (citing *United States v. Nicholson*, 955 F. Supp. 588, 592 & n.11 11 (E.D. Va. 1997)) (noting "this court knows of no instance in which 12 a court has required an adversary hearing or disclosure in 13 determining the legality of a FISA surveillance"); United States v. 14 Thomson, 752 F. Supp. 75, 79 (W.D.N.Y. 1990); United States v. 15 Mubayyid, 521 F. Supp. 2d 125, 130 (D. Mass. 2007); Rosen, 447 F. 16||Supp. 2d at 546; Kashmiri, 2010 WL 4705159, at *2-3; United States 17 v. Hassoun, 2007 WL 1068127, *4 (S.D. Fla. April 2, 2007).

As the exhibits in the Sealed Appendix make clear, there is 19 nothing extraordinary about the instant FISA-authorized electronic 20 surveillance and physical searches that would justify the 21 production and disclosure of highly sensitive and classified FISA 22 materials or the suppression of FISA-obtained or -derived evidence.

18

23

¹⁹ All citations to Jayyousi herein are to the Magistrate Judge's Report and Recommendation, which was adopted and incorporated into the Court's Opinion.

1 Here, the FISA materials are well-organized and easily reviewable 2 by the Court in camera and ex parte, and they are fully and 3 | facially sufficient to allow the Court to make an accurate 4 determination that the FISA information was lawfully acquired and 5 that the electronic surveillance and physical searches were made in 6 conformity with an order of authorization or approval. In other 7 words, the materials presented "are straightforward and readily 8 understood." In re Kevork, 634 F. Supp. 1002, 1008 (C.D. Cal. 9||1985), aff'd, 788 F.2d 566 (9th Cir. 1986). Moreover, as in other 10 cases, "[t]he determination of legality in this case is not 11 complex." Belfield, 692 F.2d at 147; see also United States v. 12|| Warsame, 547 F. Supp. 2d 982, 987 (D. Minn. 2008) (finding that the 13 "issues presented by the FISA applications are straightforward and 14 uncontroversial"); Abu-Jihaad, 531 F. Supp. 2d at 310; Thomson, 752 15 F. Supp. at 79. This Court, much like the aforementioned courts, 16 is capable of reviewing the FISA materials in camera and ex parte 17 and making the requisite legal determination without an adversarial 18 hearing.

In addition to the specific harm that would result from the 20 disclosure of the FISA materials in this case, which is detailed in 21 the classified declaration of a high-ranking FBI official in 22 support of the Attorney General's Declaration and Claim of 23 Privilege, the underlying rationale for non-disclosure is clear: 24 "In the sensitive area of foreign intelligence gathering, the need

19

for extreme caution and sometimes even secrecy may not be overemphasized." Ott, 827 F.2d at 477 ("Congress has a legitimate 3 interest in authorizing the Attorney General to invoke procedures 4 designed to ensure that sensitive security information is not 5 unnecessarily disseminated to anyone not involved in the 6 surveillance operation in question."); accord IARA, 2009 WL 5169536, at *3-4.

Confidentiality is critical to national security. 9 potentially valuable intelligence sources" believe that the United 10 States "will be unable to maintain the confidentiality of its 11 relationship to them, many [of those sources] could well refuse to 12 supply information." CIA v. Sims, 471 U.S. 159, 175 (1985); see 13 also Phillippi v. CIA, 655 F.2d 1325, 1332-33 (D.C. Cir. 1981). 14 When considering whether the disclosure of classified sources, 15 methods, techniques, or information would harm the national 16 security, federal courts have expressed a great reluctance to 17 replace the considered judgment of Executive Branch officials 18 charged with the responsibility of weighing a variety of subtle and 19 complex factors in determining whether the disclosure of 20 information may lead to an unacceptable risk of compromising the 21 intelligence gathering process, and determining whether foreign 22 agents, spies, and terrorists are capable of piecing together a 23||mosaic of information that, when revealed, could reasonably be 24 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 counterintelligence specialist who could learn much about this nation's
intelligence-gathering capabilities from what these documents
revealed about sources and methods."); Halperin v. CIA, 629 F.2d

144, 150 (D.C. Cir. 1980) ("each individual piece of intelligence
information, much like a piece of jigsaw puzzle, may aid in piecing
together other bits of information even when the individual piece
is not of obvious importance in itself"). An 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 Belfield court explained:

14

15

16

17

18

19

20

21

22

23

24

25

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

692 F.2d at 148 (footnotes and citations omitted); see also ACLU Found. of So. Cal. v. Barr, 952 F.2d 457, 465 (D.C. Cir. 1991)

1 (citing Belfield for the proposition that Section 1806(f) "is an 2 acceptable means of adjudicating the constitutional rights of 3 persons who have been subjected to FISA surveillance").

4

5

25

2. In Camera, Ex Parte Review is Constitutional

The constitutionality of FISA's in camera, ex parte review 6 provisions has been affirmed by every federal court that has considered the matter, including the Ninth Circuit. See, e.g., 8 Ott, 827 F.2d at 476-77 (FISA's review procedures do not deprive a 9 defendant of due process); Gowadia, 2009 WL 1649714, at *2; 10|| Nicholson, 2010 WL 1641167, at *3-4; Isa, 923 F.2d at 1306 11 (upholding the district court's in camera, ex parte review as 12 constitutional and stating that the process delineated under FISA 13| "provides even more protection" than defendants receive in other 14 contexts); El-Mezain, 664 F.3d at 567; Abu-Jihaad, 630 F.3d at 117; 15 Spanjol, 720 F. Supp. at 58-59; United States v. Damrah, 412 F.3d 16 618, 624 (6th Cir. 2005) ("FISA's requirement that the district 17 court conduct an ex parte, in camera review of FISA materials does 18 not deprive a defendant of due process."); Jayyousi, 2007 WL 19 851278, at *7-8; United States v. Benkahla, 437 F. Supp. 2d 541, 20||554 (E.D. Va. 2006); ACLU Foundation, 952 F.2d at 465; United 21 States v. Megahey, 553 F. Supp. 1180, 1194 (E.D.N.Y. 1982) ("ex 22 parte, in camera procedures provided in 50 U.S.C. § 1806(f) are 23 constitutionally sufficient to determine the lawfulness of the 24 electronic surveillance at issue while safequarding defendant's

fourth amendment rights"); United States v. Falvey, 540 F. Supp.

1306, 1315-16 (E.D.N.Y. 1982) (a "massive body of pre-FISA case law of the Supreme Court, [the Second] Circuit and others" supports the conclusion that the legality of electronic surveillance should be determined on an in camera, ex parte basis); Belfield, 692 F.2d at 148-49.

In summary, FISA mandates a process by which the district

court must conduct an initial in camera, ex parte review of FISA

papplications, orders, and related materials in order to determine

whether the FISA information was lawfully acquired and whether the

electronic surveillance and physical searches were made in

conformity with an order of authorization or approval. Such 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 venue in which to determine whether

the FISA information was lawfully acquired and whether the

electronic surveillance and physical searches were made in

conformity with an order of authorization or approval.

в. THE DISTRICT COURT'S SUBSTANTIVE REVIEW

2

3

10

25

Standard of Review of Probable Cause

In evaluating the legality of the FISA collection, the district court's review should determine: (1) whether the certification submitted by the Executive Branch in support of a 6||FISA application was properly made; (2) whether the application 7 established the probable cause showing required by FISA; and (3) 8 whether the collection was properly minimized. See Abu-Jihaad, 630 9|| F.3d at 130-31; see also 50 U.S.C. §§ 1806(f), 1825(g).

Although federal courts are not in agreement as to whether the 11 probable cause determinations of the FISC should be reviewed de 12 novo or accorded due deference, the material under review here 13 satisfies either standard of review. See United States v. 14 Gartenlaub, 8:14-CR-00173-CAS, Doc. No. 114, at 8 (C.D. Cal. Aug. 15 6, 2015) ([T]he Court finds that the materials that it has reviewed 16 in camera, ex parte satisfy either standard); see also Omar, slip 17 op. at 12 (2015 WL 3393825 at *7) ("[W]e have no hesitation in 18 concluding that probable cause under FISA existed under any 19 standard of review"); Abu-Jihaad, 630 F.3d at 130 ("Although the 20 established standard of judicial review applicable to FISA warrants 21 is deferential, the government's detailed and complete submissions 22 in this case would easily allow it to clear a higher standard of 23 | review."). The Government respectfully submits that it is 24 appropriate to accord due deference to the findings of the FISC,

1||but notes that a number of courts (including a judge in this 2|District), citing the ex parte nature of the proceedings, have also 3 reviewed the FISC's probable cause determination de novo. 20 While 4 in the minority, other courts have afforded due deference to the 5 findings of the FISC. Abu-Jihaad, 630 F.3d at 130; accord United 6 | States v. Ahmed, No. 1:06-CR-147, 2009 U.S. Dist. Lexis 120007 at $7 \times 21-22$ (N.D. Ga. Mar. 19, 2009) (FISC's "determination of probable 8 cause should be given 'great deference' by the reviewing court") 9 (citing *Illinois v. Gates*, 462 U.S. at 236).

In the analogous area of criminal searches and surveillance, 11||the law in the Ninth Circuit, as well as that in other federal 12 circuits, accords great deference to a magistrate judge's probable 13 cause determinations. See, e.g., United States v. Krupa, 658 F.3d 14||1174, 1177 (9th Cir. 2011); see also United States v. Smith, 581 15 F.3d 692, 694 (8th Cir. 2009); United States v. Joseph, 709 F.3d 16||1082, 1093 (11th Cir. 2013) (citing *Illinois v. Gates*, 462 U.S. at | 236); United States v. Robinson, 724 F.3d 878, 884 (7th Cir. 2013). 18 It would thus be consistent for a court that is reviewing FISA-19 authorized electronic surveillance and physical searches to adopt 20 the same posture it would when reviewing the probable cause 21 determination of a criminal search warrant issued pursuant to Rule 22 41 of the Federal Rules of Criminal Procedure. See Ahmed, 2009 23||U.S. Dist. LEXIS 120007, at *21-22 (according FISC's probable cause

29

10

24

^{20 [}CLASSIFIED MATERIAL REDACTED]

1 determinations the same deference as a magistrate's criminal 2 probable cause determination); cf. United States v. Cavanagh, 807 3 F.2d 787, 790 (9th Cir. 1987) (concluding that FISA order can be 4 considered a warrant since it is issued by a detached judicial officer and is based on a reasonable showing of probable cause).²¹

Probable Cause Standard

6

22

FISA requires a finding of probable cause that the target is a 8 foreign power or an agent of a foreign power and that each facility 9 or place at which the electronic surveillance is directed is being 10 used, or is about to be used, or that the property or premises to 11 be searched is, or is about to be, owned, used, possessed by, or is 12 in transit to or from, a foreign power or an agent of a foreign 13 power. It is this standard - not the standard applicable to 14 criminal search warrants — that this Court must apply. See 15 Cavanagh, 807 F.2d. at 790 (citing United States v. United States 16|| District Court (Keith), 407 U.S. 297, 322 (1972)); Omar, slip op. 17 at 12 (2015 WL 3393825 at *6) ("[R]ather than focusing on probable 18 cause to believe that a person has committed a crime, the FISA 19||standard focuses on the status of the target as a foreign power or 20 an agent of a foreign power.") (quoting El-Mezain, 664 F.3d at 21||564); Abu-Jihaad, 630 F.3d at 130-31; Duka, 671 F.3d at 338.

 $^{^{21}}$ Ahmed is not alone in analogizing FISA orders to search warrants. See, e.g., In re Sealed Case, 310 F.3d 717, 774 (declining to decide whether a FISA order constitutes a warrant, but noting "that to the extent a FISA order comes close to meeting Title III, that certainly 24 bears on its reasonableness under the Fourth Amendment"); but see Warsame, 547 F. Supp. 2d at 992 n.10 (noting that the need for foreign 25 intelligence justifies an exception to the warrant requirement).

1 different, and arguably lower, probable cause standard . . . 2 reflects the purpose for which FISA search orders are issued." 3 Ahmed, 2009 U.S. Dist. LEXIS 120007, at *22.

[CLASSIFIED MATERIAL REDACTED]

4

14

25

The probable cause threshold which the Government must satisfy 6||before receiving authorization to conduct electronic surveillance 7 or a physical search under FISA complies with the Fourth 8 Amendment's reasonableness standard. The argument that FISA's g different, and arguably lower, probable cause standard violates the 10 Fourth Amendment's reasonableness requirement has been uniformly 11 rejected by federal courts. See, e.g., Abu-Jihaad, 630 F.3d at 120 12 (listing sixteen cases that have ruled FISA does not violate the 13 Fourth Amendment).

The Supreme Court has stated that "[d]ifferent standards may 15 be compatible with the Fourth Amendment if they are reasonable both 16 in relation to the legitimate need of the Government for 17 intelligence information and the protected rights of our citizens." 18 Keith, 407 U.S. at 322-23 (recognizing that domestic security 19 surveillance "may involve different policy and practical 20 considerations than the surveillance of 'ordinary crime'"). 21 Keith, the Supreme Court acknowledged that: (1) the "focus of . . 22 surveillance [in domestic security investigations] may be less 23 precise than that directed against more conventional types of 24 crime; (2) unlike ordinary criminal investigations, "[t]he

1 gathering of security intelligence is often long range and involves 2 the interrelation of various sources and types of information; " and 3 (3) the "exact targets of such surveillance may be more difficult to identify" than in surveillance operations of ordinary crimes 5 under Title III. Id. Although Keith was decided before FISA's 6 enactment and addressed purely domestic security surveillance, the 7 rationale underlying Keith applies a fortiori to foreign 8 intelligence surveillance, where the Government's interest, at 9 least from a national security perspective, would typically be more 10 pronounced.

11

25

FISA was enacted partly in response to Keith. In constructing 12 FISA's framework, Congress addressed Keith's question of whether 13 departures from traditional Fourth Amendment procedures "are 14 reasonable, both in relation to the legitimate need of Government 15 for intelligence information and the protected rights of our 16 citizens," and "concluded that such departures are reasonable." 17 See S. Rep. No. 95-701, 95th Cong., 2d Sess., at 11. (1978) 18 ("Senate Report"). Similarly, many courts—including the Ninth 19 Circuit and the FISC of Review-have relied on Keith in holding that 20 FISA collection conducted pursuant to a FISC order is reasonable 21 under the Fourth Amendment. See Cavanagh, 807 F.2d at 790-91 22 (holding that FISA satisfies the Fourth Amendment requirements of 23 probable cause and particularity); In re Sealed Case, 310 F.3d at 24||738, 746 (finding that while many of FISA's requirements differ

I from those in Title III, few of those differences have 2 constitutional relevance); Duggan, 743 F.2d at 74 (holding that 3 FISA does not violate the Fourth Amendment); see also Warsame, 547 4 F. Supp. 2d at 993-94; Ning Wen, 477 F.3d 896, 898 (7th Cir. 2007) 5 (holding that FISA is constitutional despite using "a definition of 6 robable cause that does not depend on whether a domestic crime 7 has been committed"); Damrah, 412 F.3d at 625 (denying the 8 defendant's claim that FISA's procedures violate the Fourth 9 Amendment); Pelton, 835 F.2d at 1075 (finding FISA's procedures 10 compatible with the Fourth Amendment); Mubayyid, 521 F. Supp. 2d at 11 35-41 (rejecting claim that FISA violates the Fourth Amendment's 12 judicial review, probable cause, notice, and particularity 13 requirements); Falvey, 540 F. Supp. at 1311-14 (finding that FISA 14 procedures satisfy the Fourth Amendment's warrant requirement).

Standard of Review of Certifications

15

16l

25

Certifications submitted in support of a FISA application 17 should be "subject only to minimal scrutiny by the courts," Badia, 18 827 F.2d at 1463, and are "presumed valid." Duggan, 743 F.2d at 77 19 & n.6 (citing Franks v. Delaware, 438 U.S. 154, 171 (1978)); see 20 also Nicholson, 2010 WL 1641167, at *5 (quoting Rosen, 447 F. Supp. 21 2d at 545); United States v. Campa, 529 F.3d 980, 993 (11th Cir. 22||2008); United States v. Omar, Cr. No. 09-242, 2012 WL 2357734, at 23 *3 (D. Minn. June 20, 2012) ("FISA warrants are subject to 'minimal 24 scrutiny by the courts,' both upon initial presentation and

1 subsequent challenge" and that "the reviewing court must presume as 2 valid 'the representations and certifications'..."); Warsame, 547 3|| F. Supp. 2d at 990 ("a presumption of validity [is] accorded to the 4 certifications"); United States v. Sherifi, 793 F. Supp. 2d 751, 5 760 (E.D.N.C. 2011). When a FISA application is presented to the 6||FISC, "[t]he FISA Judge, in reviewing the application, is not to 7 second-guess the executive branch official's certification that the 8 objective of the surveillance is foreign intelligence information." 9 Duggan, 743 F.2d at 77. Likewise, Congress intended that the 10 reviewing district court should "have no greater authority to 11 second-guess the executive branch's certifications than has the 12 FISA judge." Id.; see also In re Grand Jury Proceedings, 347 F.3d 13||at 204-05; Badia, 827 F.2d at 1463; Rahman, 861 F. Supp. at 250; 14|| IARA, 2009 WL 5169536, at *4; Kashmiri, 2010 WL 4705159, at *1. The district court's review should determine whether the 16 certifications were made in accordance with FISA's requirements. 17 See Omar, 2012 WL 2357734, at *3 ("the reviewing court must presume 18 as valid 'the representations and certifications submitted in 19 support of an application for FISA surveillance' . . . absent a 20 showing sufficient to trigger a Franks hearing"); see also United 21 || States v. Alwan, No. 1:11-CR-13, 2012 WL 399154, at *7 (W.D. Ky.22 Feb. 7, 2012) ("the [c]ourt is not to second-guess whether the 23 certifications were correct, but merely to ensure they were 24 properly made") (quoting Ahmed, 2009 U.S. Dist. LEXIS 120007, at

15

1||*20); Campa, 529 F.3d at 993 ("in the absence of a prima facie 2 showing of a fraudulent statement by the certifying officer, 3 procedural regularity is the only determination to be made if a 4 non-United States person is the target") (quoting Badia, 827 F.2d 5||at 1463). When the target is a United States person, then the 6 district court should also ensure that each certification is not 7 "clearly erroneous." 22 Campa, 529 F.3d at 994; Duggan, 743 F.2d at 8 77; Kashmiri, 2010 WL 4705159, at *2. A "clearly erroneous" 9||finding is established only when "although there is evidence to 10 support it, the reviewing court on the [basis of the] entire 11 evidence is left with the definite and firm conviction that a 12 mistake has been committed." United States v. U.S. Gypsum Co., 333 13 U.S. 364, 395 (1948); United States v. Garcia, 413 F.3d 201, 222 14|| (2d Cir. 2005); IARA, 2009 WL 5169536, at *4 (identifying "clearly 15 erroneous" standard of review for FISA certifications).

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 in fact 20 met, the evidence obtained or derived from the FISA-authorized electronic surveillance and physical searches is, nonetheless, admissible under the "good faith" exception to the exclusionary

16

17¹

23

24

^{22 [}CLASSIFIED MATERIAL REDACTED]

rule articulated in *United States v. Leon*, 468 U.S. 897 (1984).²³

The Seventh Circuit, relying on *Leon*, held that federal officers

were entitled to rely in good faith on a FISA warrant. *Ning Wen*,

477 F.3d, at 897. As the court noted:

. 13

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

Id. (quoting Leon) (alteration in original); see also Ahmed, 2009
U.S. Dist. LEXIS 120007, at *25 n.8, 26-27 ("[t]he FISA evidence
obtained . . . would be admissible under Leon's 'good faith'
exception to the exclusionary rule were it not otherwise admissible
under a valid warrant"); Mubayyid, 521 F. Supp. 2d at 140 n.12
(applying the exception because "there appears to be no issue as to
whether the government proceeded in good faith and in reasonable
reliance on the FISA orders"); United States v. Marzook, 435 F.
Supp. 2d 778, 790-91 (N.D. Ill. 2006) (holding, in an analogous
context, that "the FBI's reliance on the Attorney General's
approval under Executive Order No. 12333 - an order that no court
has found unconstitutional - was [] objectively reasonable because
that order pertains to foreign intelligence gathering.").

^{23 &}quot;[E]ven if we were to conclude that amended FISA is unconstitutional, evidence derived from it would nevertheless have been admissible in the government's case. . . The exclusionary rule precludes the admission of evidence tainted by a Fourth Amendment violation" only in those cases where its application will deter police misconduct. Duka, 671 F.3d at 346 (citing Leon, 468 U.S. at 918).

1

21

22

23

24

25

The FISA-authorized electronic surveillance and physical searches at issue in this case, authorized by a duly enacted 3 statute and an order issued by a neutral judicial officer, would 4 fall squarely within this "good faith exception." There is no basis to find that any declarations or certifications at issue in 6 this case were deliberately or recklessly false. See Leon, 468 $7 \parallel \text{U.S.}$ at 914-15; see also Massachusetts v. Sheppard, 468 U.S. 981 (1984); United States v. Canfield, 212 F.3d 713, 717-18 (2d Cir. 9 2000). Further, there are no facts indicating that the FISC failed 10||to act in a neutral and detached manner in authorizing the 11 electronic surveillance and physical searches at issue. Leon, 468 12 U.S. at 914-15. Moreover, as the Court will see from its in 13 camera, ex parte review of the FISA materials, facts establishing 14 the requisite probable cause were submitted to the FISC, the FISC's 15 orders contained all of the requisite findings, and "well-trained 16 officers" reasonably relied on those orders. Therefore, in the 17 event that the Court questions whether a particular FISC order was 18 supported by sufficient probable cause, the information obtained 19 pursuant to those orders would be admissible under Leon's "good 20 faith exception to the exclusionary rule.

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

[CLASSIFIED MATERIAL REDACTED]

A. THE INSTANT FISA APPLICATIONS MET FISA'S PROBABLE CAUSE STANDARD

1	[CLASSIFIED MATERIAL REDACTED]
2	1. [CLASSIFIED MATERIAL REDACTED]
3	[CLASSIFIED MATERIAL REDACTED]
4	2. [CLASSIFIED MATERIAL REDACTED]
5	[CLASSIFIED MATERIAL REDACTED]
6	a. [CLASSIFIED MATERIAL REDACTED]
7	[CLASSIFIED MATERIAL REDACTED]
8	i. [CLASSIFIED MATERIAL REDACTED]
9	[CLASSIFIED MATERIAL REDACTED]
10	ii. [CLASSIFIED MATERIAL REDACTED]
11	[CLASSIFIED MATERIAL REDACTED]
12	iii. [CLASSIFIED MATERIAL REDACTED]
13	[CLASSIFIED MATERIAL REDACTED]
14	iv. [CLASSIFIED MATERIAL REDACTED]
15	[CLASSIFIED MATERIAL REDACTED]
16	V. [CLASSIFIED MATERIAL REDACTED]
17	[CLASSIFIED MATERIAL REDACTED]
18	b. [CLASSIFIED MATERIAL REDACTED]
19	[CLASSIFIED MATERIAL REDACTED]
20	i. [CLASSIFIED MATERIAL REDACTED]
21	[CLASSIFIED MATERIAL REDACTED]
22	ii. [CLASSIFIED MATERIAL REDACTED]
	[CLASSIFIED MATERIAL REDACTED]
23	iii. [CLASSIFIED MATERIAL REDACTED]
24	[CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED] 1 [CLASSIFIED MATERIAL REDACTED] 2 V. [CLASSIFIED MATERIAL REDACTED] 3 [CLASSIFIED MATERIAL REDACTED] 3. The FISC Correctly Concluded that the Targeted 5 Facilities or Places Were Being Used, or Were About to Be Used, by the Targets of the 6 Electronic Surveillance and that the Targeted Premises or Property Were, or Were About to Be Owned, Used, Possessed by or in Transit to or from, the Targets of the Physical Searches 8 [CLASSIFIED MATERIAL REDACTED] 9 a. [CLASSIFIED MATERIAL REDACTED] 10 [CLASSIFIED MATERIAL REDACTED] 11 i. [CLASSIFIED MATERIAL REDACTED] 12 [CLASSIFIED MATERIAL REDACTED] 13 ii. [CLASSIFIED MATERIAL REDACTED] 14 [CLASSIFIED MATERIAL REDACTED] 15 iii. [CLASSIFIED MATERIAL REDACTED] 16 [CLASSIFIED MATERIAL REDACTED] 17 iv. [CLASSIFIED MATERIAL REDACTED] 18 [CLASSIFIED MATERIAL REDACTED] 19 V. [CLASSIFIED MATERIAL REDACTED] 20 [CLASSIFIED MATERIAL REDACTED] 21 vi. [CLASSIFIED MATERIAL REDACTED] 22 [CLASSIFIED MATERIAL REDACTED] 23 [CLASSIFIED MATERIAL REDACTED] 24 i. [CLASSIFIED MATERIAL REDACTED] 25

1	[CLASSIFIED MATERIAL REDACTED]
2	ii. [CLASSIFIED MATERIAL REDACTED]
3	[CLASSIFIED MATERIAL REDACTED]
4	iii. [CLASSIFIED MATERIAL REDACTED]
5	[CLASSIFIED MATERIAL REDACTED]
6	$i_{oldsymbol{V}}.$ [CLASSIFIED MATERIAL REDACTED]
7	[CLASSIFIED MATERIAL REDACTED]
8	c. Conclusion: There Was Sufficient Probable Cause to Establish that the Information
9	Acquired from the Targeted Facilities, Places, Property, or Premises Was Lawfully
10	Acquired
11	[CLASSIFIED MATERIAL REDACTED]
12	B. THE CERTIFICATIONS COMPLIED WITH FISA
13	[CLASSIFIED MATERIAL REDACTED]
14	1. Foreign Intelligence Information
15	[CLASSIFIED MATERIAL REDACTED]
16	2. <u>"A Significant Purpose"</u>
17	[CLASSIFIED MATERIAL REDACTED]
18	3. Information Not Reasonably Obtainable Through
19	Normal Investigative Techniques
20	[CLASSIFIED MATERIAL REDACTED]
21	C. ELECTRONIC SURVEILLANCE AND PHYSICAL SEARCHES WERE
	CONDUCTED IN CONFORMITY WITH AN ORDER OF AUTHORIZATION OR APPROVAL
22	
23	[CLASSIFIED MATERIAL REDACTED]
24	

1. The Standard Minimization Procedures

Once a reviewing court is satisfied that the electronic 3 surveillance or physical searches were properly certified and the 4 information was lawfully acquired pursuant to FISA, it must then 5 examine whether the electronic surveillance or physical searches 6 were lawfully conducted. See 50 U.S.C. §§ 1806(e)(2), 7 1825(f)(1)(B). In order to examine whether the electronic 8 surveillance or physical searches were lawfully conducted, the 9 reviewing court must determine whether the Government followed the 10 relevant minimization procedures to appropriately minimize the 11 information acquired pursuant to FISA.

[CLASSIFIED MATERIAL REDACTED]

1

2

12

13l

25

FISA's legislative history and the applicable case law 14 demonstrate that the definitions of "minimization procedures" and 15 "foreign intelligence information" were intended to take into 16 account the realities of collecting foreign intelligence because 17 the activities of persons engaged in clandestine intelligence 18 gathering or international terrorism are often not obvious on their 19 face. See Rahman, 861 F. Supp. at 252-53. The degree to which 20 information is required to be minimized varies somewhat given the 21 specifics of a particular investigation, such that less 22 minimization at acquisition is justified when "the investigation is 23 focusing on what is thought to be a widespread conspiracy" and more 24 extensive surveillance is necessary "to determine the precise scope

```
1 of the enterprise." In re Sealed Case, 310 F.3d at 741; see also
 2 United States v. Bin Laden, 126 F. Supp. 2d 264, 286 (S.D.N.Y.
 3 2000) ("more extensive monitoring and greater leeway in
 4 minimization efforts are permitted in a case like this given the
 5 world-wide, covert and diffuse nature of the international
 6 terrorist group(s) targeted" [internal quotation marks omitted]).
 7 || Furthermore, the activities of foreign powers and their agents are
 8 often not obvious from an initial or cursory overhear of
 9 conversations. To the contrary, agents of foreign powers
10 frequently engage in coded communications, compartmentalized
11 operations, the use of false identities and other practices
12 designed to conceal the breadth and aim of their operations,
13 organization, activities and plans. See, e.g., United States v.
14|| Salameh, 152 F.3d 88, 154 (2d Cir. 1998) (noting that two
15 conspirators involved in the 1993 bombing of the World Trade Center
16 in New York referred to the bomb plot as the "study" and to
17 terrorist materials as "university papers"). As one court
18 explained, "[i]nnocuous-sounding conversations may in fact be
19 signals of important activity; information on its face innocent
20 when analyzed or considered with other information may become
21 critical." Kevork, 634 F. Supp. at 1017 (quoting H.R. Rep. No. 95-
22 1283, 95th Cong., 2d Sess., Pt. 1, at 55 (1978) (hereinafter "House
23||Report")); see also Hammoud, 381 F.3d at 334 (citing Salameh, 152
24||F.3d at 154); In re Sealed Case, 310 F.3d at 740-41; Thomson, 752
```

1 F. Supp. at 81 (noting that it is permissible to retain and 2 disseminate "bits and pieces" of information until the 3||information's "full significance becomes apparent") (citing House 4 Report, part 1, at 58); Bin Laden, 126 F. Supp. 2d at 286. 5 Likewise, "individual items of information, not apparently 6 significant when taken in isolation, may become highly significant 7 when considered together over time." Rahman, 861 F. Supp. at 252-8 53 (citing House Report, part 1, at 55, 59). The Government must 9 be given flexibility where the conversations are carried out in a 10||foreign language. Mubayyid, 521 F. Supp. 2d at 134; Rahman, 861 F. 11 Supp. at 252. As a result, "courts have construed 'foreign 12 intelligence information' broadly and sensibly allowed the 13 government some latitude in its determination of what is foreign 14 intelligence information." Rosen, 447 F. Supp. 2d at 551.

The nature of the foreign intelligence information sought also 16 impacts implementation of the minimization procedures at the 17 retention and dissemination stages. There is a legitimate need to 18 conduct a thorough post-acquisition review of FISA information that 19 involves a United States person who is acting as an agent of a 20 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

21

22

23

24

it is determined that they are not involved in the clandestine intelligence activities and may have to be disseminated in order to determine their innocence.

House Report, part 1, at 58. Indeed, at least one court has cautioned that, when a U.S. 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.

Cf. id. at 81 (quoting House Report part 1, at 58). Accordingly, to pursue leads, Congress intended that the Government be given "a significant degree of latitude" with respect to the "retention of information and the dissemination of information between and among counterintelligence components of the Government." Cf. id.

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, 95th Cong., 2d Sess., 39 (quoting United States v. Bynum, 485 F.2d 490, 500 (2d Cir. 1973)) ("Senate Report"). The Fourth Circuit reached the same conclusion in Hammoud, stating that the "mere fact that innocent conversations were recorded, without more, does not

1 establish that the government failed to appropriately minimize 2 surveillance." 381 F.3d at 334.

Accordingly, in reviewing the adequacy of minimization 4 efforts, the test to be applied is neither whether innocent 5 conversations were intercepted, nor whether mistakes were made with 6 respect to particular communications. Rather, as the United States 7 | Supreme Court stated in the context of Title III surveillance, 8 there should be an "objective assessment of the [agents'] actions 9 in light of the facts and circumstances confronting [them] at the 10||time." Scott v. United States, 436 U.S. 128, 136 (1978). 11 test of compliance is 'whether a good-faith effort to minimize was 12 made.'" Mubayyid, 521 F. Supp. 2d at 135; see also Hammoud, 381 13 F.3d at 334 ("[t]he minimization requirement obligates the 14 Government to make a good faith effort to minimize the acquisition 15 and retention of irrelevant information"); Senate Report at 39-40 16 (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 18 and have done all they reasonably could do to avoid unnecessary 19 intrusion"); IARA, 2009 WL 5169536, at *6 (quoting Senate Report at 20||39-40).

Moreover, as noted above, FISA expressly states that the 22 Government is not required to minimize information that is 23 "evidence of a crime," whether or not it is also foreign 24 intelligence information. 50 U.S.C. §§ 1801(h)(3), 1821(4)(c); see

21

| also Isa, 923 F.2d at 1304 (noting that "[t]here is no requirement that the 'crime' be related to foreign intelligence"). As a 3 result, to the extent that certain communications of a United 4 States person may be evidence of a crime or otherwise may establish 5 an element of a substantive or conspiratorial offense, such 6 communications need not be minimized. See id. at 1305.

Even in the limited occasions described herein, when certain 8 communications were not properly minimized, suppression would not 9 be the appropriate remedy with respect to those communications that 10 met the standard. Cf. United States v. Falcone, 364 F. Supp. 877, 11||886-87 (D.N.J. 1973), aff'd, 500 F.2d 1401 (3d Cir. 1974) (Title 12 III). As discussed above, absent evidence that "on the whole" 13|| there has been a "complete" disregard for the minimization 14 procedures, the fact that some communications should have been 15||minimized does not affect the admissibility of others that were 16 properly acquired and retained. Indeed, Congress specifically 17 intended that the only evidence that should be suppressed is the 18 "evidence which was obtained unlawfully." House Report at 93. 19 FISA's legislative history reflects that Congress intended only a 20 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.

21

22

23

24

Id.; see also Falcone, 364 F. Supp. at 886-87; accord United States

v. Medunjanin, No. 10-CR-19-1, 2012 WL 526428, at *12 (E.D.N.Y.

Feb. 16, 2012) (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 collections discussed herein. Consequently, for the reasons stated above, the Court should find that the FISA collections discussed herein were lawfully conducted under the minimization procedures approved by the FISC and applicable to the FISA collections discussed herein.

V. THE COURT SHOULD REJECT THE DEFENDANTS' LEGAL ARGUMENTS

In their motions, the defendants present numerous arguments in support of their request for the suppression of FISA-obtained or -derived evidence and the disclosure of the FISA materials. Their arguments essentially fall into two categories: (1) that the FISA-obtained or -derived evidence should be suppressed for several reasons, including because the applications "may" have contained intentional or reckless material falsehoods or omissions and "may" not have established probable cause, and the FISA procedural requirements "may" not have been met; and (2) that disclosure of the FISA materials is both necessary for them to litigate suppression issues, and is required by due process considerations.

 $1 \mid (Doc. 69, at 1-3; Doc. 70, at 5-6)$ For the reasons set forth below and as the Court will see in its ex parte, in camera review of the 3||FISA materials, these arguments are without merit.

A. THE DEFENDANTS HAVE NOT ESTABLISHED ANY BASIS FOR THE COURT TO SUPPRESS THE FISA INFORMATION

In support of their request for suppression, the defendants claim that the FISA applications "may" have: (1) failed to establish probable cause; 24 (2) contained intentional or reckless falsehoods or omissions; (3) not included the required certifications, including that a significant purpose was the collection of foreign intelligence information; and (4) not contained or implemented the requisite minimization procedures. 25 (Doc. 69, at 10-16; Doc. 70, at 17-22) This Court should deny each of these arguments, for the reasons discussed below.

1. The Government Satisfied the Probable Cause Requirements of FISA

[CLASSIFIED MATERIAL REDACTED] 26

5

10

11

12

13

14

15

16

17

18

[[]CLASSIFIED MATERIAL REDACTED]

²⁵ At the outset, the defendants argue that their burden in seeking 19 suppression of FISA information "must be relaxed," based on a case, United States v. Moussaoui, addressing neither suppression nor FISA. F.3d 453, 472 (4th Cir. 2004). Moussaoui, in which the Fourth Circuit addressed the defendant's Sixth Amendment right to compulsory process, is simply inapplicable to the standard for suppression under FISA.

²⁶ Defendant Elhuzayel argues for *de novo* review by this Court of 22| the FISA materials, or even a review "more exacting than the FISC's review," (Doc. 70, at p. 27), a position that has no basis in the law. 23 However, the Government respectfully submits that the Court will find that the FISA information was lawfully acquired and that the electronic surveillance and physical searches were made in conformity with an order of authorization or approval, under either de novo review or a due deference review.

Third, the defendants suggest that the FISA applications may 2 have contained "raw intelligence," which may not have been "reliable and/or had a verifiable track record, or was [not] independently corroborated." (Doc. 69, at 12-13; Doc. 70, at 18-5|19) The defendants do not define "raw intelligence," and the only 6 case they cite - a dissenting opinion in an appeal from a 7 Guantanamo habeas proceeding - does not support their position. 8 See Latif v. Obama, 666 F.3d 746, 755-56 (D.C. Cir. 2011) (Tatel, J., dissenting) (noting that intelligence reports are not 10 "necessarily unreliable. Perhaps after careful scrutiny district 11 courts will conclude that many are reliable.") In a similar case, 12 the D.C. Circuit found no basis for "a per se rule that information 13 contained in an intelligence report is inherently unreliable." 14|| Barhoumi v. Obama, 609 F.3d 416, 429 (D.C. Cir. 2010). To the 15 contrary, such information need only "be presented in a form, or 16 with sufficient additional information, that permits . . . [the] |17| court to assess its reliability." Id. (quoting Parhat v. Gates, 18||532 F.3d 834, 847, 849 (D.C. Cir. 2008)) ("[W]e do not suggest that 19 hearsay evidence is never reliable."). The same is true in the 20 more analogous context of criminal search warrants. In making 21 probable cause determinations based on a totality of the 22 circumstances, courts routinely review information presented in 23 search warrant affidavits for indicia of reliability or independent corroboration. See Illinois v. Gates, 462 U.S. 213, 238 (1983)

1 (probable cause sufficient, based on totality of the circumstances,
2 where anonymous informant's recitation of detailed facts was
3 corroborated by police observation); Draper v. United States, 358
4 U.S. 307, 313 (1959) (probable cause sufficient where hearsay
5 information from previously reliable source was corroborated by
6 independent police investigation); United States v. Martinez7 Garcia, 397 F.3d 1205, 1216-17 (9th Cir. 2005) (probable cause
8 sufficient where reliable informant told police he had purchased
9 drugs from defendant, and police observed three controlled drug
10 buys).

[CLASSIFIED MATERIAL REDACTED]

2. <u>Franks v. Delaware Does Not Require Suppression</u> of FISA Materials

The defendants allege that the FISA applications "may" contain intentional or reckless falsehoods or omissions, in contravention of Franks v. Delaware, 438 U.S. 154 (1978), and requests that the Court conduct a Franks hearing. (Doc. 69, at 16-19; Doc. 70, at 22-25) 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 5||false statement was 'necessary' to the FISA Judge's approval of the 6 application." Duggan, 743 F.2d at 77 n.6 (quoting Franks, 438 U.S. at 155-56). A defendant must show that the agent lied or recklessly disregarded the truth with specific evidence in the form of "[a]ffidavits or sworn or otherwise reliable statements of 10 witnesses." Franks, 438 U.S. at 171. The Franks threshold is not 11 met even by an offer of proof of an impropriety that might have 12 affected the outcome of the probable cause determination, but 13 rather requires one that was "necessary to the finding of probable 14 cause." United States v. Colkley, 899 F.2d 297, 301-02 (4th Cir. 15||1990); see also United States v. Shnewer, 2008 U.S. Dist. LEXIS 16 112001, at 38 (D. N.J. Dec. 29, 2009) ("[E] ven if the Court were to 17 determine there existed a reckless or intentional falsehood or 18 omission in the FISA application materials, the evidence obtained 19 still should not be suppressed unless the Court makes the further 20 finding that the falsehood or omission was material to the probable 21 cause determination.").

[CLASSIFIED MATERIAL REDACTED] 27

22

²⁴ 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

1

21

Nonetheless, the defendants claim that a Franks hearing and 2 disclosure to them of the FISA materials "are necessary in order to 3 permit [the defendants] the opportunity to prove that the affiants 4 before the FISC intentionally or recklessly made materially false 5 statements and omitted material information from the FISA 6 applications," (Doc. 69, at 18-19; Doc. 70, at 25), an approach 7 which would allow them, and defendants in every case, to obtain the 8 FISA materials by merely alleging some impropriety. 28 Disclosing 9 FISA materials to defendants would then become the rule, violating 10 Congress' clear intention, set forth in 50 U.S.C. §§ 1806(f) and 11 1825(g), that the FISA materials be reviewed in camera and ex parte 12 in a manner consistent with the realities of modern intelligence 13 needs and investigative techniques. Courts have acknowledged that 14||the FISA statute does not envision such disclosure without 15 establishing a basis for it. For instance, the Daoud court noted 16 that it was "hard" for a defendant to make the Franks showing 17 "without access to the classified [FISA] materials," but the 18 "drafters of [FISA] devised a solution: the judge makes the initial 19 determination, based on full access to all classified materials. .

20|| . ." Daoud, 755 F.3d at 483-84. Similarly, in Belfield, the court

information were included. Franks, 438 U.S. at 171; Colkley, 899 F.2d at 22||300; United States v. Ketzeback, 358 F.3d 987, 990 (8th Cir. 2004); United States v. Martin, 615 F.2d 318, 328 (5th Cir. 1980).

²⁸ A judge in this District referred to this as "backwards reasoning" in denying a defendant's motion to suppress FISA-derived 24 evidence. United States v. Mihalik, 11-CR-833(A), Doc. No. 108, at 2 (C.D. Cal., Oct. 3, 2012) (Minute Order Denying Defendant's Motion to 25 Suppress FISA-Derived Evidence).

1 noted that "Congress was also aware of these difficulties [faced by defense counsel without access to FISA materials and] chose to 3 resolve them through means other than mandatory disclosure." Belfield, 692 F.2d at 148. Judge Leinenweber framed the difficulty 5 facing defense counsel:

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

Kashmiri, 2010 U.S. Dist. LEXIS 119470, at *17.

6

7

8

9

10

11

12

21

25

Courts have rejected other defendants' attempts to force a 13 Franks hearing by positing unsupported speculation to challenge the $^{14}\parallel$ validity of FISC orders, and this Court should do so here. See ||Abu-Jihaad|, 531 F. Supp. 2d at 309; Hassoun, 2007 WL 1068127 at *4; Mubayyid, 521 F. Supp. 2d at 130-31; Kashmiri, 2010 U.S. Dist. LEXIS 119470, at *17 (noting that the court "has already undertaken $^{18}\parallel$ a process akin to a *Franks* hearing through its *ex parte*, *in camera* |19| review"); Shnewer, 2008 U.S. Dist. LEXIS 112001, at 37 ("This 20| catch-22 has not troubled courts, however, and they defer to FISA's statutory scheme."); Mubayyid, 521 F. Supp. 2d at 131 ("The balance ||22|| struck under FISA - which is intended to permit the gathering of 23 foreign intelligence under conditions of strict secrecy, while providing for judicial review and other appropriate safeguards -

1 would be substantially undermined if criminal defendants were 2 granted a right of disclosure simply to ensure against the 3 possibility of a Franks violation.").

The defendants have failed to carry the burden of establishing the prerequisites for a Franks hearing, and their attempt to obtain 6 disclosure of the FISA materials to meet that burden is 7 unprecedented and runs counter to FISA, Franks, and the intent of 8 Congress. For these reasons, the Court should therefore deny the 9 defendants' request for a Franks hearing and his request for 10 suppression of the FISA information.

The Certifications Complied with FISA 3.

The defendants submit that the certifications "may" not have 13 included the required certifications, such as that foreign intelligence information was a significant purpose of the 15 collection, that the information sought was foreign intelligence 16 information, and that the information cannot reasonably be obtained by normal investigative techniques. (Doc. 69, at 19-20; Doc. 70, 18 at 25-26) This claim has also been consistently denied by the courts. See, e.g., Hammoud, 381 F.3d at 333.

[CLASSIFIED MATERIAL REDACTED] 29

11

12

20

21

22

²⁹ FISA's "significant purpose" standard was held unconstitutional in Mayfield, a civil case, which was eventually vacated by the Ninth 23 Circuit on the ground that the plaintiff lacked standing. See Mayfield v. United States, 588 F.3d 1252 (9th Cir. 2009). And, as is the case for the lower court's decision in Mayfield, when a judgment is vacated by a higher court "it deprives the [lower] court's opinion of precedential effect." Los Angeles County v. Davis, 440 U.S. 625, 634 n. 6 (1979).

4. The Government Complied with the Minimization Procedures

[CLASSIFIED MATERIAL REDACTED] 30

1

2

3

8

9

10

11

12

13

14

15

21

25

As the Court will see from its ex parte, in camera review of the FISA materials, 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.

в. THE DEFENDANTS HAVE NOT ESTABLISHED ANY BASIS FOR THE COURT TO DISCLOSE FISA MATERIALS

In support of their argument for disclosure of the FISA materials, the defendants claim that disclosure: (1) "may be 'necessary' under § 1806(f);" (2) is required under § 1806(g) and due process; and (3) required by the adversary system of justice.

[CLASSIFIED MATERIAL REDACTED]

³⁰ In their motions, the defendants incorrectly paraphrase Section 1801(h). (Doc. 69, at 20-21; Doc. 70, at 26-27) First, the defendants state that the procedures "ensure that surveillance is reasonably designed to minimize the acquisition and retention of private information regarding people who are being wiretapped;" instead, Section 1801(h)(1) defines procedures (instead of the surveillance) "that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the 19 dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United 20||States to obtain, produce, and disseminate foreign intelligence information." 50 U.S.C. § 1801(h)(1).

Second, the defendants state that the procedures "prevent dissemination of non-foreign intelligence information," whereas the 22 statute requires that "nonpublicly available information, which is not foreign intelligence information, . . . shall not be disseminated in a 23 manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance." 50 U.S.C. § 1801(h)(2).

 $1 \mid (Doc. 69, at 21-26; Doc. 70, at 27-33)$ For the following reasons, 2 the Court should deny the request for disclosure.

1. Disclosure is Not "Necessary" under FISA

31

11

12

18

The defendants assert that "there are ample justifications for 5 disclosure of the FISA applications," which would permit defense 6 counsel an opportunity to identify procedural irregularities and to 7 demonstrate that the defendants' knowledge was lacking, the 8 defendants' activities fell within the protection of the First 9 Amendment, and the information in the applications was unreliable 10 or obtained via illegal means. 31 (Doc. 69, at 22; Doc. 70, at 28)

³¹ Defendant Badawi notes that "although [he] does not currently possess security clearance . . . counsel is certain that the government 13 could assist in that process. (Doc. 70, at 28) Federal courts have consistently rejected such arguments when ruling on defense requests for disclosure of FISA materials. For example, in Ott, the Ninth Circuit found a similar argument unpersuasive, stating that "Congress has a legitimate interest in authorizing the Attorney General to invoke 15 procedures designed to ensure that sensitive security information is not unnecessarily disseminated to anyone not involved in the surveillance 16 operation in question, whether or not she happens for unrelated reasons to enjoy security clearance." Ott, 827 F.2d at 477 (emphasis in |17|| original); accord El-Mezain, 664 F.3d at 568; Warsame, 547 F. Supp. 2d at 989 n.5.

The defendants also note that the Court could "issue an appropriate Protective Order . . . that would provide elaborate protection for 19 CLASSIFIED information, and which would permit CLASSIFIED materials to be disclosed to defense counsel but not to the [defendants]." (Doc. 69, at 20 | 22; Doc. 70, at 28) If this Court concludes from its in camera, exparte review of the FISA materials that it is capable of accurately determining the legality of the FISA collection at issue, then no defense attorney, even one with an otherwise appropriate security clearance, would have a "need to know" any of the FISA materials, and no defense attorney would be entitled to see them. See Executive Order 13526, §§ 4.1(a), 6.1(dd), 75 Fed.Reg. 707, 720, 729 (Jan. 5, 2010), which requires that a "need to 23 know" determination be made prior to the disclosure of classified information to anyone, including those who possess an appropriate 24 security clearance. In Baldrawi v. Dep't of Homeland Security, 596 F. Supp. 2d 389, 400 (D. Conn. 2009), the court determined that even counsel 25|| who held a top secret security clearance did not have a "need to know,"

As the Court is aware, these claims are not unique to this case, and, as detailed above, each of the claims was raised in support of suppression. The defendants, then, are seeking disclosure to bolster their arguments for suppression, which is not permissible under the statute.

There is only one reason to disclose the FISA materials to 7 defense counsel. The Court must conduct its review of those 8 materials in camera and ex parte, and disclosure is within the 9 Court's discretion only following that review and only if the Court 10 is unable to determine the legality of the electronic surveillance, 11 physical searches, or both, without the assistance of defense 12 counsel. 50 U.S.C. §§ 1806(f), 1825(g); Rosen, 447 F. Supp. 2d at 13 546; Daoud, 755 F.3d at 482; Duggan, 743 F.2d at 78. This holding 14||is fully supported by the legislative history of Section 1806(f), 15 which states: "The court may order disclosure to [the defense] only 16 if it finds that such disclosure is necessary to make an accurate determination of the legality of the surveillance . . . Once a 18|| judicial determination is made that the surveillance was lawful, a 19 motion for discovery . . . must be denied." Senate Report at 64-20 65; see also Hassan, 742 F.3d at 138 (where the court "emphasized 21| that, where the documents 'submitted by the government [are] 22 sufficient' to 'determine the legality of the surveillance,' the 23||FISA materials should not be disclosed.") (quoting Squillacote, 221

and therefore denied him access to classified documents. Accord United States v. Amawi, 2009 WL 961143, at *1 (N.D. Ohio, Apr. 7, 2009).

 $1 \parallel F.3d$ at 554). As this Court will see from its review, the FISA 2 materials are presented in a well-organized and straightforward 3 manner that will allow the Court to make its determination of the 4 lawfulness of the FISA collection without input from defense 5 counsel.

The defendants' request, which effectively calls for 7 disclosure where defense counsel could provide assistance, instead 8 of where necessary, is merely an attempt to circumvent the clear 9 language of the statute. See 50 U.S.C. §§ 1806(f), 1825(g). As 10 the Belfield court stated: "Congress was adamant, in enacting FISA, 11 that [its] 'carefully drawn procedure[s]' are not to be bypassed." 12 692 F.2d at 146 (citing Senate Report at 63); see also United 13 States v. Mohamud, 2014 WL 2866749, *32 (D. Or., June 24, 2014) 14 ("Obviously it would be helpful to the court to have defense 15 counsel review the materials prior to making arguments. Congress, 16 however, did not put 'helpful' in the statute; it chose 17 'necessary.'"). As the Daoud Court stated, "the defendant's 18 misreading of the statute" would circumvent the required in camera, 19 ex parte review whenever a defense counsel "believed disclosure 20 necessary, since if the judge does not conduct the ex parte review, 21 she will have no basis for doubting the lawyer's claim of 22 necessity." 755 F.3d at 842.

The defendants are not entitled to the FISA materials for the 24 purpose of challenging the lawfulness of the FISA authorities, as

23

1||FISA's plain language precludes defense counsel from accessing the 2 classified FISA materials to conduct a fishing expedition. 3 Medunjanin, the court noted that "[d]efense counsel . . . may not 4 inspect the FISA dockets to construct a better argument for 5 inspecting the FISA dockets. Such a circular exercise would be 6 patently inconsistent with FISA " 2012 WL 526428 at *10. 7 See Badia, 827 F.2d at 1462 (rejecting the defendant's request for 8 "disclosure of the FISA application, ostensibly so that he may 9 review it for errors"); Mubayyid, 521 F. Supp. 2d at 131.

10

24

25

The defendants have failed to present any colorable basis for 11 disclosure, as this Court is able to review and make a 12 determination as to the legality of the FISA collection without the 13 assistance of defense counsel. Where, as here, defense 14 participation is not necessary, FISA requires that the FISA 15 materials remain protected from disclosure. Congress' clear 16 intention is that FISA materials should be reviewed in camera and 17 ex parte and in a manner consistent with the realities of modern 18 intelligence needs and investigative techniques. There is simply 19 nothing extraordinary about this case that would prompt this Court 20 to order the disclosure of highly sensitive and classified FISA 21 materials. See Rosen, 447 F. Supp. 2d at 546 ("exceptional nature 22 of disclosure of FISA material is especially appropriate in light 23 of the possibility that such disclosure might compromise the

1 ability of the United States to gather foreign intelligence 2 information effectively") (citing Belfield, 692 F.2d at 147).

3

21

2. Due Process Does Not Require Disclosure

The defendants also claim that they are entitled to disclosure of the FISA materials under 50 U.S.C. § 1806(g) and the Due Process 6 Clause of the Fifth Amendment. (Doc. 69, at 23; Doc. 70, at 29) Courts are in agreement, however, that FISA's in camera, ex parte review does not violate the due process clause of the Fifth 9 Amendment, nor does due process require that defendants be granted |10| access to the FISA materials except as provided for in 50 U.S.C. $11 \parallel SS = 1806(f)$, (g) and 1825(g), (h). See, e.g., Ott, 827 F.2d at 476-|77; Gowadia, 2009 WL 1649714, at st2; ACLU Foundation, 952 F.2d at 13||465; Nicholson, 955 F. Supp. at 592 (The court found that based on "the unanimous holdings of prior case law, . . . that FISA does not 15 violate the Fifth or Sixth Amendments by authorizing ex parte in 16 camera review."); Benkahla, 437 F. Supp. 2d at 554; El-Mezain, 664 | 17 | | F.3d | at 567; Abu-Jihaad, 630 F.3d at 117; Spanjol, 720 F. Supp. at 18 58-59; Damrah, 412 F.3d at 624; Jayyousi, 2007 WL 851278, at *7-8; 19 Megahey, 553 F. Supp. at 1194; Falvey, 540 F. Supp. at 1315-16; 20 Belfield, 692 F.2d at 148-49; Nicholson, 2010 WL 1641167, at *3-4. The plain intention of § 1806(q) - allowing the Court to order 22 disclosure of material to which the defendants would be entitled 23 under the Due Process Clause, such as material that had not been 24 previously disclosed under Brady, even while ruling against the

25 defendants' motions generally - cannot be interpreted to support

the defendants' demand for access to all of the FISA materials in advance of the Court's in camera, ex parte review and determination of the legality of the collection. The necessity of disclosing FISA materials is a factual, not a legal, question. With respect to any claim that the FISA materials contain information that due process requires be disclosed to the defense, the request is premature since the Court will make that factual determination for itself during its in camera, ex parte review. The Government is confident that the Court's review of the challenged FISA materials will not reveal any material that due process requires be disclosed to the defendants, such as Brady material, as provided for in \$ 1806(g). Accordingly, the defendants' claim that they are entitled to the disclosure of the FISA material under Section 14 1806(q) and due process should be rejected.

3. The Adversary System Does Not Require Disclosure

Finally, the defendants claim that they are entitled to disclosure because the lack thereof "would render the proceedings . . . ex parte," and thus "antithetical to the adversary system that is the hallmark of American criminal justice." (Doc. 69, at 23; Doc. 70, at 29) This claim is contrary to all of the relevant case law (as opposed to the case law cited

³² "If the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure." 50 U.S.C. §§ 1806(g) and 1825(h).

1 by the defense, all of which predates FISA or does not address 2||FISA). Several courts, including District Courts in the Ninth 3 Circuit, have addressed the right to confrontation in this context 4 and found that "FISA's in camera review provisions have been held 5| to be constitutional." Nicholson, 2010 U.S. Dist. LEXIS 45126 6 (citing Isa, 923 F.2d at 1307-08 (Sixth Amendment right of 7 confrontation is not violated by FISA's in camera review 8 procedure)); see also United States v. Lahiji, 2013 WL 550492 (D. 9 Or. Feb. 12, 2013), *4 (Court found no violation of defendants' 10 Fourth, Fifth, or Sixth Amendment rights); United States v. Jamal, 11 2011 U.S. Dist. LEXIS 12224 (D. Az. Feb. 11, 2011), *5 (movant's 12 Sixth Amendment rights were not violated by trial counsel's 13 inability to discuss FISA materials); United States v. Hussein, 14||2014 U.S. Dist. LEXIS 59400 (S.D. Cal. Apr. 29, 2014), *3 (The "in 15 camera, ex parte review process under FISA satisfies due process 16 under the United States Constitution."); Falvey, 540 F. Supp. at 17 1315-16 (rejecting First, Fifth, and Sixth Amendment challenges and 18 noting that a "massive body of pre-FISA case law of the Supreme 19 Court, Circuit and others" supports the conclusion that the 20 | legality of electronic surveillance should be determined on an in 21 camera, ex parte basis); Nicholson, 955 F. Supp. at 592 ("Based on 22| the unanimous holdings of prior case law, . . . FISA does not 23 violate . . . the Sixth Amendment[] by authorizing ex parte in 24 camera review."); Benkahla, 437 F. Supp. 2d at 554.

Courts have also consistently rejected similar arguments challenging FISA under the Sixth Amendment. See Lahiji, 2013 WL 3 550492, *4; Warsame, 547 F. Supp. 2d at 988 n.4 (finding argument "without merit") (citing Nicholson, 955 F. Supp. at 592); Belfield, 5 692 F.2d at 148; Isa, 923 F.2d at 1306-07; Megahey, 553 F. Supp. at 6 1193. In overturning a district court's order to disclose FISA 7 materials to the defense, the Daoud Court described the belief that 8 adversary procedure is always essential to resolve contested 9 issues of fact" as "an incomplete description of the American legal 10 system in general and the federal judicial system in particular." 11 755 F.3d at 482.

The defendant's arguments in support of disclosure of the FISA 13 materials have no basis in the law, and disclosure of the FISA 14 materials would cause exceptionally grave damage to the national 15 security. The Government respectfully submits that, contrary to 16|| the defendants' assertions, there is nothing extraordinary about 17 this case to justify an order to disclose the highly sensitive and 18 classified FISA materials in this case under the applicable FISA 19 standard. See Rosen, 477 F. Supp. 2d at 546 ("Review of the FISA 20 applications, orders and other materials in this case presented 21 none of the concerns that might warrant disclosure to the 22 defense."). Accordingly, the defendants' motions for disclosure of 23 the FISA materials should be denied.

24

1

VI. CONCLUSION: THERE IS NO BASIS FOR THE COURT TO DISCLOSE THE FISA MATERIALS OR TO SUPPRESS THE FISA INFORMATION

The defendants' motions should be denied. FISA's provisions for in camera, ex parte review comport with the due process requirements of the United States Constitution. See, e.g., El-Mezain, 664 F.3d at 567; Abu-Jihaad, 630 F.3d at 117; Spanjol, 720 F. Supp. at 58-59; United States v. Damrah, 412 F.3d at 624. The defendants advance no argument to justify any deviation from these well-established precedents.

The Attorney General has filed a declaration in this case stating that disclosure or an adversary hearing would harm the national security of the United States. Therefore, FISA mandates that this Court conduct an in camera, ex parte review of the challenged FISA materials to determine whether the information was lawfully acquired and whether the electronic surveillance and physical searches 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

1 Court finds that disclosure is necessary to the Court's accurate 2 determination of the legality of the FISA collection.

The Government respectfully submits that the Court can make 4 this determination without disclosing the classified and highly sensitive FISA materials to the defendants. The FISA materials at 6 issue here are organized and readily understood, and an overview of 7 them has been presented herein as a frame of reference. This Court 8 will be able to render a determination based on its in camera, ex 9 parte review, and the defendants have failed to present any 10 colorable basis for supplanting Congress' reasoned judgment with a 11 different proposed standard of review.

Furthermore, the Court's examination of the FISA materials in 13||the Sealed Appendix will demonstrate that the Government satisfied 14||FISA's requirements to obtain orders for electronic surveillance 15 and physical searches, that the information obtained pursuant to 16 FISA was lawfully acquired, and that the electronic surveillance 17 and physical searches were made in conformity with an order of 18 authorization or approval.

Even if this Court were to determine that the acquisition of 20 the FISA information had not been lawfully acquired or that the 21 electronic surveillance and physical searches were not made in 22 conformity with an order of authorization or approval, the FISA 23 evidence would nevertheless be admissible under the "good faith" 24 exception to the exclusionary rule articulated in Leon, 468 U.S.

19

3

 $1 \parallel 897 \pmod{1984}$. See also Ning Wen, 477 F.3d at 897 (holding 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 5|| 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 searches at issue in this case were both lawfully authorized and 9 lawfully conducted; (2) hold that disclosure of the FISA materials 10 and the Government's classified submissions to the defendants is 11 not authorized because the Court is able to make an accurate determination of the legality of the surveillance without disclosing the FISA materials or any portions thereof; (3) hold that the fruits of electronic surveillance and physical searches 15|| should not be suppressed; (4) deny the defendants' motions without 16 an evidentiary hearing; and (5) order that the FISA materials and 17 the Government's classified submissions be maintained under seal by

12

13

18

19

20

21

22

23

24

1 the Classified Information Security Officer or his or her 2 designee. 33 3 DATED: March 10, 2016 Respectfully submitted, EILEEN M. DECKER United States Attorney PATRICIA A. DONAHUE Assistant United States Attorney Chief, National Security Division /s/ JUDITH A. HEINZ DEIRDRE Z. ELIOT Assistant United States Attorneys Central District of California 10 /s/ 11 MICHAEL DITTOE Trial Attorney 1.5 Counterterrorism Section National Security Division 13 United States Department of Justice /s/ 14 PURVI PATEL Attorney Advisor 15 Office of Intelligence National Security Division 16 United States Department of Justice 17 Attorneys for Plaintiff UNITED STATES OF AMERICA 18 19 33 A district court order granting motions or requests under 50 20 U.S.C. § 1806(g), a decision that electronic surveillance was not lawfully authorized or conducted, and an order requiring the disclosure

23

²¹ of FISA materials is a final order for purposes of appeal. 50 U.S.C. § 1806(h). Should the Court conclude that disclosure of any item within 22 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.