UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF KENTUCKY
BOWLING GREEN DIVISION
CASE NO. 1:11-CR-13-R

UNITED STATES OF AMERICA **PLAINTIFF**

v.

WAAD RAMADAN ALWAN and
MOHANAD SHAREEF HAMMADI **DEFENDANTS**

MEMORANDUM OPINION AND ORDER

This matter is before the Court upon the Defendants' Motion to Compel Disclosure of Evidence Obtained Under Foreign Intelligence Surveillance Act and to Suppress Same.[1] Docket Number ("DN") 22. In response, the Government filed both a classified and an unclassified Memorandum in Opposition to Defendants' Motion. DN 47 (unclassified response).[2] On December 21, 2011, Defendant Alwan changed his plea from not guilty to guilty on all counts charged in his indictment. DN 55. Because Alwan has pled guilty, this memorandum opinion and order addresses the Motion to Compel and Suppress only so far as it pertains to Defendant Hammadi. For the following reasons, Hammadi's motion is DENIED.

BACKGROUND

Defendant Mohanad Shareef Hammadi ("Hammadi") is an Iraqi citizen who was granted refugee status under the Refugee Admissions Program and entered the United States in July of 2009.[3] During all times pertinent to his indictment, Hammadi lived in Bowling Green,

[1] The Motion to Compel and Suppress was originally filed by Defendant Alwan. Defendant Hammadi orally joined the motion in a telephonic conference held before the Court on June 21, 2011. DN 38.
[2] All references to the Government's response are to the unclassified memorandum.
[3] For the purposes of the Foreign Intelligence Surveillance Act ("FISA") and the discussion below, the Court finds that Hammadi is not a "United States Person" as that term is defined by FISA. *See* 50 U.S.C. §§ 1801(i) and 1821(1). FISA prescribes certain additional requirements when electronic surveillance or a physical search will involve a "United States Person." These additional requirements are not applicable in the present case because Hammadi is an Iraqi citizen, and even though he entered the United States as a refuge under the Refugee

Kentucky. On May 25, 2011, Hammadi was arrested and charged with ten counts of participating in terrorism-related offenses. DN 6. Specifically, Hammadi is charged with five separate counts of violating 18 U.S.C. § 2339A (providing material support to terrorists), four separate counts of violating 18 U.S.C. § 2339B (providing material support or resources to designated foreign terrorist organizations), and one count of violating 18 U.S.C. § 2332g (missile systems designed to destroy aircraft). *Id.*

On May 31, 2011, the Government filed notice, pursuant to 50 U.S.C. §§ 1806(c) and 1825(d), that it intended to offer evidence against Hammadi obtained via electronic surveillance and/or physical search authorized under the Foreign Intelligence Surveillance Act of 1978 ("FISA"), as amended, 50 U.S.C. §§ 1801 *et seq.*[4] DN 19. After receiving this notice, Hammadi moved this Court, pursuant to 50 U.S.C. § 1806(e) and 1825(f), to disclose and suppress such evidence on the basis that it was illegally obtained or not collected in conformity with the order of the Foreign Intelligence Surveillance Court ("FISC").

The Government opposes disclosure and suppression, and along with its memorandum in opposition, it invoked the *in camera* and *ex parte* review procedures provided in 50 U.S.C. §§ 1806(f) and 1825(g). Pursuant to those statutory provisions, the Government filed the affidavit of the United States Attorney General, stating that any disclosure of the FISA materials would harm the national security of the United States. DN 47-1. After receiving such an affidavit, the Court "shall . . . review *in camera* and *ex parte* the application, order, and such other material relating to the surveillance [or physical search] as may be necessary to determine whether the

---

Admissions Program, he has never been a citizen of the United States and there has been no showing that his refugee status has been adjusted to that of permanent alien resident.

[4] The FISA statutes are generally divided into two broad categories: 1) electronic surveillance, 50 U.S.C. §§1801-1812, and 2) physical searches, 50 U.S.C. §§ 1821-1829. For the purposes of clarity and efficiency, the Court, when addressing both electronic surveillance and physical searches, will list the pertinent electronic surveillance sections first, followed by the corresponding physical search statutes. When dealing with electronic surveillance or physical searches separately, the Court will highlight the relevant statutory distinctions.

surveillance [or physical search] of the aggrieved person was lawfully authorized and conducted." 50 U.S.C. §§ 1806(f) and 1825(g). Thus, in order to address Hammadi's motion to disclose and suppress, the Court was required by statute, as the result of the Attorney General's affidavit, to conduct an *in camera* and *ex parte* review of the FISA materials. As described below, the Court's review of the evidence revealed that it was legally obtained and all applications and orders were properly made and issued. The FISA materials pertaining to Hammadi will not be disclosed or suppressed.

DISCUSSION

I. Overview of Foreign Intelligence Surveillance Act.

The Foreign Intelligence Surveillance Act of 1978 ("FISA" or "the Act") prescribes the methods whereby the Government may conduct electronic surveillance and physical searches of a "foreign power"[5] or "agent of a foreign power"[6] after a high-ranking official certifies that a "significant purpose"[7] of the search is to collect "foreign intelligence information."[8]

a. Role of the Courts.

Under FISA, the Chief Justice of the United States is required to designate eleven U.S. District Court judges to sit on the Foreign Intelligence Surveillance Court ("FISC"). 50 U.S.C. § 1803(a)(1). Judges of the FISC are tasked with hearing applications for and granting (or denying) orders for electronic surveillance and physical searches aimed at gathering foreign intelligence information. 50 U.S.C. §§ 1803(a)(1) and 1822(b). The Chief Justice is also required to designate three judges to serve on the Foreign Intelligence Surveillance Court of Review ("FISCR"). 50 U.S.C. § 1803(b). The FISCR reviews any FISC denial of an application

[5] "Foreign power" is defined in 50 U.S.C. §§ 1801(a) and 1821(1).
[6] "Agent of a foreign power" is defined in 50 U.S.C. §§ 1801(b) and 1821(1).
[7] *See* 50 U.S.C. §§ 1804(a)(6)(B) and 1823(a)(6)(B).
[8] "Foreign intelligence information" is defined in 50 U.S.C. §§ 1801(e) and 1821(1).

for search or surveillance. *Id.* Additionally, the U.S. District Courts are authorized to review the legality of electronic surveillance and physical searches upon the motion of an "aggrieved person."[9] 50 U.S.C. §§ 1806(f), 1825(g).

b. The FISA Application.

Before the Government is authorized to conduct electronic surveillance or a physical search, it must obtain an order from a FISA judge. To obtain a FISA order, the Government must file an application with the FISC. No order will issue unless an application is properly made. 50 U.S.C. §§ 1804 and 1823 set out the elements that must be present in an application for electronic surveillance or physical search.

i. Application for Electronic Surveillance Order - 50 U.S.C. § 1804.

An application for electronic surveillance presented to a FISA judge must be made in writing by a federal officer and be approved by the Attorney General. 50 U.S.C. § 1804(a). The electronic surveillance application must include: 1) the identity of the federal officer making the application; 2) the identity of the target of the electronic surveillance; 3) a statement of the facts relied upon by the person making the application to justify his belief that the target is a foreign power or 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 agent of a foreign power; 4) a statement of proposed minimization procedures; 5) a description of the nature of the information sought and the type of communications or activities subjected to surveillance; 6) a certification by a high-ranking official; 7) a summary statement describing how the surveillance will be effected and whether physical entry is required to effect surveillance; 8) a statement of facts concerning all previous applications that have been made to any FISA judge

[9] An "aggrieved person" is defined in 50 U.S.C. §§ 1801(k) and 1821(2) and includes anyone who was the subject of electronic surveillance or whose premises or property was subject to a physical search.

involving any of the persons, facilities, or places that are the subject of the current application; and 9) a statement of the period of time for which the electronic surveillance is required to be maintained. 50 U.S.C. § 1804(a)(1)-(9).

ii. Application for a Physical Search Order - 50 U.S.C. § 1823.

The elements that must be contained in an application for a physical search are substantially similar to those required for an electronic surveillance application. An application for a physical search presented to a FISA judge must be made in writing by a federal officer and be approved by the Attorney General. 50 U.SC. § 1823(a). The physical search application must include: 1) the identity of the federal officer making the application; 2) the identity of the target as well as a description of the premises or property to be searched and the information, material, or property to be seized, reproduced, or altered; 3) a statement of the facts relied upon by the applicant to justify his belief that the target of the physical search is a foreign power or an agent of a foreign power, the premises to be searched contains foreign intelligence information, and the premises to be search is or is about to be owned, used, or possessed by, or is in transit to or from, a foreign power or agent of a foreign power; 4) a statement of proposed minimization procedures; 5) a statement of the nature of the foreign intelligence sought and the manner in which the physical search is to be conducted; 6) a certification by a high-ranking official; 7) if the search involves the residence of a "United States person,"[10] a statement by the Attorney General describing previous efforts to obtain the foreign intelligence information; and 8) a statement of facts concerning any previous applications made to any FISA judge involving the person, premises, or property that are the subject of the current application. 50 U.S.C. §

[10] "United States person" is defined in 50 U.S.C. §§ 1801(i) and 1821(1) and is, for the purposes of this opinion, any U.S. citizen or alien lawfully admitted for permanent residence. The FISA distinctions involving a "United States person" are not relevant in this case because Hammadi, as an Iraqi citizen and refugee, is not a "United States person" within the terms of the statute.

1823(a)(1)-(8).

iii. Statement of Proposed Minimization Procedures - 50 U.S.C. §§ 1804(a)(4) and 1823(a)(4).

As stated above, an application to the FISA court for an order authorizing electronic surveillance or physical search must be accompanied by a statement of proposed minimization procedures. 50 U.S.C. § 1804(a)(4) and 1823(a)(4). In general, "minimization procedures" are specific procedures:

> Reasonably designed in light of the purposes and technique of the particular surveillance [or physical search], 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) and 1821(4)(A). Thus, every FISA application must contain a statement detailing the minimization procedures that will be used during the electronic surveillance or physical search which will prevent the acquisition, retention, and dissemination of information collected concerning unconsenting United States persons. "Minimization procedures" must also "allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes." 50 U.S.C. §§ 1801(h)(3) and 1821(4)(C).

iv. Certification by a High-Ranking Official - 50 U.S.C. §§ 1804(a)(6) and 1823(a)(6).

In addition to minimization procedures, an application to the FISC for an order authorizing electronic surveillance or physical search must be accompanied by the certification of a high-ranking official. 50 U.S.C. § 1804(a)(6) and 1823(a)(6). More specifically, the high-ranking official must be one of the individuals listed in the statute,[11] and the actual certification

[11] For the purposes of the certification, the high-ranking official must be "the Assistant to the President for National Security Affairs, an executive branch official or officials designated by the President from among those executive

must state that: 1) the official deems the information sought to be foreign intelligence information; 2) a significant purpose of the search is to obtain foreign intelligence information; 3) such information cannot be obtained by normal investigative techniques; and 4) the foreign intelligence information sought is one of the categories of information described in the definition of "foreign intelligence information."[12] 50 U.S.C. §§ 1804(a)(6) and 1823(a)(6). Furthermore, the certification must contain a statement of the basis for the official's belief that the information sought is a specific category of foreign intelligence information and why it cannot be obtained by normal investigative techniques. 50 U.S.C. §§ 1804(a)(6)(E) and 1823(a)(6)(E).

If the FISA application for electronic surveillance or physical search contains the information listed in 50 U.S.C. §§ 1804 and 1823, then the FISA judge must determine whether to issue an order authorizing the surveillance or search.

c. The FISA Order.

Once the Government submits a proper application to the FISC for electronic surveillance or physical search, a FISA judge may issue the requested order only after making certain statutory findings.

i. Necessary Findings for Issuance of a FISA Order - 50 U.S.C. §§ 1805(a) and 1824(a).

To issue an order, a FISA judge must find that: 1) the application has been made by a federal officer and approved by the Attorney General; 2) on the basis of the facts submitted with the application, there is probable cause to believe that the target of the electronic surveillance or physical search is a foreign power or agent of a foreign power and that the facilities or places subject to the electronic surveillance, or the property or premises to be searched, is being used, or

---

officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate, or the Deputy Director of the Federal Bureau of Investigations, if designated by the President as a certifying official . . . ." 50 U.S.C. §§ 1804(a)(6) and 1823(a)(6).

[12] *See* 50 U.S.C. § 1801(e).

is about to be used, owned, or possessed by, or is in transit to or from a foreign power or an agent of a foreign power; 3) the proposed minimization procedures meet the definition of minimization procedures; 4) and the application filed contains all of the statements and certifications required by the electronic surveillance or physical search application statutes. 50 U.S.C. §§ 1805(a)(1)-(4) and 1824(a)(1)-(4). Only after making these findings may the FISA judge issue the requested order.

ii. Required Components of a FISA Order for Electronic Surveillance or Physical Search - 50 U.S.C. § 1805(c) and 1824(c).

Once a FISA judge makes the required statutory findings, an order for electronic surveillance or physical search may issue. The order, itself, must comply with the FISA statutes and contain certain specifications and directions.

1. FISA Order Specifications - 50 U.S.C. §§ 1805(c)(1) and 1824(c)(1).

In the case of electronic surveillance, a FISA order must specify: 1) the identity of the target; 2) the nature and location of the facilities at which the electronic surveillance will be directed; 3) the type of information sought to be acquired and the type of communications subject to the surveillance; 4) the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance; and 4) the time period during which electronic surveillance is approved. 50 U.S.C. § 1805(c)(1)(A)-(E).

For a physical search, a FISA order must specify: 1) the identity of the target; 2) the nature and location of the premises or property to be searched; 3) the type of information, material, or property to be seized, altered, or reproduced; 4) a statement of the manner in which the physical search is to be conducted and, if there is more than one physical search authorized, the authorized scope of each search and what minimization procedures apply to each; and 5) the

period of time during which the physical searches are approved. 50 U.S.C. § 1824(c)(1)(A)-(E).

2. FISA Order Directions - 50 U.S.C. §§ 1805(c)(2) and 1824(c)(2).

In addition to certain specification, a FISA order for electronic surveillance must contain certain statutorily-required directions. A FISA order authorizing electronic surveillance must direct that: 1) the minimization procedures be followed; 2) any third-party providing the target with certain services[13] must assist the Government in accomplishing the electronic surveillance with minimal interference with the services provided to the target; 3) any records concerning the surveillance kept by the third-party must be maintained according to procedures approved by the Attorney General; and 4) the Government must compensate the third-party for aiding in the surveillance. 50 U.S.C. § 1805(c)(2)(A)-(D).

For a physical search, the FISA order must direct that: 1) the minimization procedures be followed; 2) any third-party providing the target with certain services must give the Government access to all information, facilities, and assistance necessary to accomplish the physical search in a way that will protect the secrecy of the search and provide minimal interference with the services provided to the target; 3) any records concerning the search kept by the third-party must be maintained according to procedures approved by the Attorney General; 4) the Government must compensate the third-party for aiding in the physical search; and 5) the federal officer conducting the physical search must promptly report to the court the circumstances and results of the physical search. 50 U.S.C. § 1824(c)(2)(A)-(E).

iii. The Probable Cause Standard for Issuance of a FISA Order.

No FISA order authorizing electronic surveillance or physical search can issue unless a

[13] Third-parties providing "certain services" to the target include, but are not limited to, communications providers, landlords, custodians possessing items for the target, and common carriers. *See* 50 U.S.C. §§ 1805(c)(2)(B) and 1824(c)(2)(B).

FISA judge makes a specific finding that there is probable cause to believe that the target of the surveillance or search is a foreign power or agent of a foreign power and that the facilities or property subject to the surveillance or search is or is about to be owned, used, possessed, or is in transit to or from a foreign power or agent of a foreign power. 50 U.S.C. §§ 1805(a)(2) and 1824(a)(2). This probable cause standard is different than the probable cause standard applicable to a criminal arrest or search warrants. "The showing necessary under the Fourth Amendment to justify surveillance conducted for national security purposes is not necessarily analogous to the standard of probable cause applicable to criminal investigations." *United States v. Cavanagh,* 807 F.2d 787, 790 (9th Cir. 1987) (citing *United States v. United States District Court*, 407 U.S. 297, 322 (1972)). FISA's probable cause standard has repeatedly been held to be constitutional. *See, e.g., United States v. Isa*, 923 F.2d 1300, 1304 (8th Cir. 1991); *Cavanagh*, 807 F.2d at 790-91; *United States v. Duggan*, 743 F.2d 59, 72-74 (2d Cir. 1984).

d. Review of FISA Applications and Orders by the District Court.

If authorized by the United States Attorney General, information derived from FISA surveillance and searches may be used in subsequent criminal prosecutions. 50 U.S.C. §§ 1806(b) and 1825(c). Before the FISA materials may be introduced, however, the Government must provide notice to the court and to the party against whom the evidence will be introduced. 50 U.S.C. §§ 1806(c) and 1825(d). Once receiving notice that the Government intends to use FISA materials, the "aggrieved party" - the party against whom the surveillance or search was conducted - may move to suppress the evidence based on the grounds that: 1) the information was unlawfully acquired; or 2) the electronic surveillance or physical search did not conform to the order authorizing the action. 50 U.S.C. §§ 1806(e) and 1825(f). The motion to suppress must be made to the district court in which the matter is pending, and that district court has the

jurisdiction to determine whether the surveillance or search was illegal or not in conformity with the order of the FISC. 50 U.S.C. §§ 1806(f) and 1825(g). Once the district court receives a motion to suppress FISA materials, the court may address the motion as it would in any other criminal case unless the Attorney General files an affidavit declaring that disclosure of the evidence or an adversarial hearing on the motion would harm the national security of the United States. 50 U.S.C. §§ 1806(f) and 1825(g).

If the Attorney General files such an affidavit, the district court is required to "review *in camera* and *ex parte* the application, order, and such other materials relating to the surveillance [or physical search] as may be necessary to determine whether the surveillance [or physical search] of the aggrieved person was lawfully authorized and conducted." 50 U.S.C. §§ 1806(f) and 1825(g). When reviewing the FISA materials *in camera* and *ex parte*, the district court may disclose the applications, orders, or other materials related to the surveillance or search to the aggrieved person "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) and 1825(g). Thus, the statutory provisions of FISA make it clear that when a motion to suppress by the defendant is followed by the affidavit of the Attorney General, *in camera* and *ex parte* review of the FISA materials is the rule, and disclosure of any such evidence to the criminal defendant is the exception. *See United States v. Belfield*, 692 F.2d 141, 147 (D.C. Cir. 1982) ("The language [of the FISA statutes] clearly anticipates that an *ex parte, in camera* determination is to be the rule. Disclosure and an adversary hearing are the exception, occurring *only* when necessary.") Disclosure should only take place where the court is unable to make an accurate determination as to the legality of the evidence. If the court can make an accurate determination without disclosure to the defendant, then the FISA materials should not be disclosed.

i. Standards of Review Applied to FISA Applications and Orders.

Upon a defendant's motion to suppress and upon the Attorney General's affidavit requiring *in camera* and *ex parte* review, the district court must determine the legality of the FISA surveillance or search. FISA surveillance or search is only legal if it is the product of a proper FISA application, a proper FISA order, and the surveillance and/or search complies with the order. When determining whether the FISA application and order were properly made, the district court applies the following standards of review.

1. Standard of Review Applicable to FISA Applications.

The Government must apply to the FISC before being issued a FISA order for surveillance or search. A FISA application for electronic surveillance or physical search must contain the items listed in 50 U.S.C. §§ 1804 and 1823, respectively. Upon a defendant's motion to suppress, the district court must review the application to determine whether it was properly made.

A FISA application is subject only to minimal scrutiny upon review. *See United States v. Abu-Jihaad*, 630 F.3d 102, 130 (2d Cir. 2010). Where a statutory application "was properly made and earlier approved by a FISA judge, it carries a strong presumption of veracity and regularity in a reviewing court." *Pelton*, 835 F.2d at 1076 (citing *Duggan*, 743 F.2d at 77). When reviewing an application, the district court must ensure that the application contains all of the requirements listed in 50 U.S.C. §§ 1804 and 1823. In reviewing the procedural check list, the court's emphasis will naturally fall on the requirement that the application be accompanied by the certification of a high-ranking official. 50 U.S.C. §§ 1804(6) and 1823(6).

Like the application itself, the "certification is . . . subjected to only minimal scrutiny by the courts." *Duggan*, 743 F.2d at 77. The certification is used to ensure that a significant

purpose of the surveillance or search is to obtain foreign intelligence information. 50 U.S.C. §§ 1804(a)(6)(B) and 1823(a)(6)(B). The FISA judge, reviewing the initial application "is not to second-guess the executive branch official's certification that the objective of the surveillance is foreign intelligence information." *Duggan*, 743 F.2d at 77. Similarly, "when a person affected by a FISA surveillance [or search] challenges the FISA Court's order, a reviewing court is to have no greater authority to second-guess the executive branch's certifications than has the FISA Judge . . . ." *Id.* "The [c]ourt is not to second-guess whether the certifications were correct, but merely to ensure they were properly made." *United States v. Ahmed*, 1:06-cr-147-WSD-GGB, 2009 U.S. Dist. LEXIS 120007, at *20 (N.D. Ga. March 19, 2009). In all, the Government's application for a FISA order, and the certification of a high-ranking official accompanying it, are given substantial deference and only receive minimal scrutiny when reviewed by the district court.

2. Standard of Review Applicable to FISA Orders.

Upon a defendant's motion to suppress pursuant to 50 U.S.C. §§ 1806(e) and 1825(f), a district court must also review the FISA order authorizing the surveillance or search. As an initial matter, a FISA order authorizing electronic surveillance or physical search must contain the components mandated by statute in 50 U.S.C. §§ 1805 and 1824, respectively. Most importantly, the FISA order must contain a finding of probable cause by the FISA judge that the target of the surveillance or search is a foreign power or agent of a foreign power and that the facilities or places at which the surveillance is directed or the premises or property to be searched is or is about to be owned, used, possessed by, or is in transit to or from a foreign power or agent of a foreign power. 50 U.S.C. §§ 1805(a)(2) and 1824(a)(2). Unlike the FISA application, however, the FISA judge's probable cause determination is reviewed *de novo* by the district

court upon a defendant's motion to suppress. *See United States v. Hammoud*, 381 F.3d 316, 332 (4th Cir. 2004), *rev'd on other grounds*, 543 U.S. 1097 (2005); *United States v. Kashmiri*, 09-CR-830-4, 2010 U.S. Dist. LEXIS 119470, at *4 (N.D. Ill. Nov. 10, 2010); *United States v. Nicholson*, 09-CR-40-BR, 2010 U.S. Dist. LEXIS 45126, at *13 (D. Or. April 20, 2010); *United States v. Warsame*, 547 F. Supp. 2d 982, 990-91 (D. Minn. 2008); *United States v. Rosen*, 447 F. Supp. 2d 538, 545 (E.D. Va. 2006).

II. Analysis of the Legality of the FISA Materials in the Present Case.

Defendant Hammadi has moved pursuant to 50 U.S.C. §§ 1806(e) and 1825(f) to disclose and suppress all FISA applications and orders and any evidence derived from or relating to any electronic surveillance or physical searches conducted against him as authorized by order of the FISC. The Government opposes Hammadi's motion and has filed an affidavit of the United States Attorney General declaring that any disclosure of or hearing on these matters will harm the national security of the United States. As a result of the Attorney General's affidavit, the Court conducted an *in camera, ex parte* review of the FISA materials that the Government indicated could be used in Hammadi's criminal prosecution. Based on that review, the Court finds that: 1) the FISA applications complied with the statutory requirements, 2) the FISA orders contained the statutory requirements and were based on probable cause, and 3) the actual electronic surveillance and physical searches were conducted in compliance with the orders of the FISC.

1. Review of the FISA Applications.

A district court reviews applications for FISA electronic surveillance or physical search using minimal scrutiny. In the present case, the Court has reviewed the applications the Government presented to the FISC for electronic surveillance and physical search. Upon review,

the Court finds that each application contained the requirements set forth in 50 U.S.C. § 1084 and 1823. Most importantly for the statutory requirements, the Court finds that the applications contained a statement of the proposed minimization procedures and a certification by a high-ranking official. The proposed minimization procedures are those previously proposed by the Attorney General and approved of by the FISC.[14] The certifications by high-ranking officials show that Government demonstrated that a "significant purpose"[15] of the surveillance or search was to obtain "foreign intelligence information." Overall, the FISA applications for electronic surveillance or physical search complied with the FISA application statutes. As such, the Court finds no error in the applications or accompanying certifications, and where the applications are procedurally accurate, the Court's inquiry is complete.

a. Hammadi has failed to offer proof that would require a *Franks* hearing.

Hammadi has challenged the FISA applications in this case based on a violation of *Franks v. Delaware*, 438 U.S. 154 (1978).[16] A *Franks* challenge allows a criminal defendant "to challenge the truthfulness of factual statements made in an affidavit supporting [a] warrant[.]" *Id.* at 155. In the present case, Hammadi alleges that the FISA applications for electronic surveillance or physical search contain false statements that were deliberately or recklessly made. He argues that a *Franks* hearing, followed by disclosure and suppression, is required to

[14] The Attorney General's proposed minimization procedures were submitted to the Court along with the other FISA materials for *in camera* and *ex parte* review. After review of the procedures, the Court finds that the minimization procedures comply with the definition of that term found in 50 U.S.C. §§ 1801(h) and 1821(4).

[15] Hammadi has not challenged the validity of the "significant purpose" standard required to be shown in the certification of a high-ranking official. Hammadi has merely argued that the certification did not show that a significant purpose was to obtain foreign intelligence information. The Court points out that the "significant purpose" test has repeatedly been held to be constitutional. *See, e.g., United States v. Abu-Jihaad*, 630 F.3d 102, 128-29 (2d Cir. 2010); In re *Sealed Cases*, 310 F.3d 717, 746 (F.I.S. Ct. Rev. 2002).

[16] The rule from *Franks* is applicable in the FISA context because "[t]he due process underpinnings of *Franks* . . . apply to the government's process of obtaining a FISA order." *Kashmiri*, 2010 U.S. Dist. LEXIS 119470, at *15 (citing *Duggan*, 743 F.2d at 77 n.6).

remedy any evidence obtained as a result of the false statements made in the FISA applications.[17]

In order to assert a *Franks* violation, a criminal defendant must make a "substantial preliminary showing" that: 1) "a false statement knowing and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit," and 2) "the allegedly false statement is necessary to the finding of probable cause . . . ." *Id.* at 155-56. In order to raise a *Franks* challenge, "the challenger's attack must be more than conclusory. . . . There must be allegations of deliberate falsehood or of reckless disregard for the truth, and those allegations must be accompanied by an offer of proof." *Id.* at 171. It is insufficient for a defendant to alleged negligence or innocent mistake. *Id.* Finally, even if these requirements are met, and the "material that is subject of the alleged falsity or reckless disregard is set to one side, [and] there remains sufficient content in the warrant affidavit to support a finding of probable cause, no hearing is required." *Id.* at 171-72.

A defendant bears a heavy burden when asserting a *Franks* challenge. Not only must the defendant offer proof that an affiant's false statements were deliberately or recklessly made, he must show that there could have been no probable cause finding absent those statements. In the present case, Hammadi cannot offer any proof that statements in the FISA applications were false or were deliberately or recklessly made because Hammadi has not been able to examine the applications. The Court is cognizant of the substantial difficulties Hammadi has encountered in trying to assert a *Franks* violation. Regardless of the difficulties, however, it does not change the evidentiary burdens he must meet. Other courts have encountered this same problem in the FISA context and have held that absent a specific offer of proof, no *Franks* violation can be established. As stated in *Kashmiri*:

[17] A warrant and a FISA order for surveillance or search are treated analogously for a *Franks* analysis. *See United States v. Ning Wen*, 477 F.3d 896, 897-98 (7th Cir. 2006).

> A defendant in a case that involves a FISA order . . . does not automatically receive a *Franks* hearing. Rather, the FISA order challenger must make a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included in the FISA application, as well as establish that the allegedly false statement was necessary for the FISC to approve the application. Failure to satisfy either of these prongs proves fatal to a *Franks* hearing request.
>
> . . . .
>
> The Court recognizes the frustrating position from which Defendant must argue for a *Franks* hearing. *Franks* provides an important Fourth Amendment safeguard to scrutinize the underling basis for probable cause in a search warrant. The requirements to obtain a hearing, however, are seemingly unattainable by Defendant. He does not have access to any of the materials concerning the FISA application or surveillance; all he has is notice that the government plans to use this evidence against him.
>
> 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 material 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 *15-17 (citations omitted). In the present case, Hammadi has failed to offer "substantial proof" that the statements underlying the FISA applications were false and deliberately or recklessly made. Thus, his request for a hearing fails the first prong of *Franks*. Because of Hammadi's failure to show substantial proof, the Court finds that he is not entitled to a *Franks* hearing, and his request is denied.

2. Review of the FISA Orders.

An order of the FISC authorizing electronic surveillance or a physical search must contain the necessary findings, specifications, and directions contained in 50 U.S.C. § 1805 and 1824. Upon a defendant's motion to suppress, the reviewing court must ensure that the FISA orders contain the statutory prerequisites. Additionally, and most importantly, the district court must review *de novo* the probable cause determination required by 50 U.S.C. §§ 1805(a)(2) and

1824(a)(2) to determine whether probable cause existed for issuance of the FISA order for surveillance or search.

In the present case, the Court, as part of its *in camera* and *ex parte* review of the FISA materials, has examined all the FISA orders pertaining to Hammadi that were submitted by the Government. From the review, the Court finds that the orders complied with the procedural requirements set forth in 50 U.S.C. §§ 1805 and 1824, and contained the necessary findings, specifications, and directions required by those sections.

Most importantly the Court finds that, after a *de novo* review of the facts submitted with the FISA applications, there was probable cause to believe that Hammadi was "an agent of a foreign power" and that each of the facilities, places, premises, or property at which the electronic surveillance or physical search was directed was, or was about to be owned, used, possessed by, or was in transit to or from Hammadi. *See* 50 U.S.C. §§ 1805(a)(2) and 1824(a)(2). Thus, Hammadi's arguments based on the Government's failure to demonstrate probable cause are without merit. The FISA orders contained the elements required by statute and issued upon a finding of probable cause.

3. Collection of Evidence Complied with the FISA Orders and was Lawfully Conducted.

As a final argument in favor of disclosure and suppression of the FISA materials, Hammadi argues that the electronic surveillance and physical searches were not conducted in conformity with the FISA orders authorizing such surveillance or search. Having found that the FISA applications and orders were properly made, the Court has reviewed the FISA-obtained or -derived evidence. The Court finds no indication that the evidence was collected in violation of the FISA orders. The Government followed the governing minimization procedures and meticulously followed the orders of the FISC when collecting the evidence. The Court finds that

any electronic surveillance or a physical search was lawfully conducted and any evidence collected from such surveillance or search was collected in compliance with the governing FISA orders. As such, Hammadi's argument that the Government failed to comply with the FISA orders and the surveillance or search was not lawfully conducted is without merit.

CONCLUSION

Defendant Mohanad Shareef Hammadi has moved the Court to disclose and suppress the FISA materials that may be used against him in the pending criminal prosecution. For the foregoing reasons, Defendant's motion is **DENIED**.

Thomas B. Russell, Senior Judge
United States District Court

February 7, 2012