EXHIBIT T

PUBLIC UNCLASSIFIED BRIEF

No. 06-36083
(Consolidated with Nos. 06-17132, 06-17137)

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

AL-HARAMAIN ISLAMIC FOUNDATION, INC., et al.,
Plaintiffs - Appellees,

v.

GEORGE W. BUSH, et al.,
Defendants - Appellants.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

BRIEF FOR APPELLANTS

PAUL D. CLEMENT
Solicitor General

GREGORY G. GARRE
Deputy Solicitor General

DARYL JOSEFFER
Assistant to the Solicitor General

PETER D. KEISLER
Assistant Attorney General

DOUGLAS N. LETTER
THOMAS M. BONDY
ANTHONY A. YANG
Attorneys, Appellate Staff
Civil Division, Room 7513
U.S. Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530
Telephone: (202) 514-3602

STATEMENT OF THE ISSUE

Plaintiffs, a terrorist organization and two lawyers affiliated with it, contend that they were subjected to warrantless electronic surveillance under the now-discontinued Terrorist Surveillance Program ("TSP"). The district court recognized that the Government had properly invoked the state secrets privilege, and that it remains secret whether plaintiffs were actually subject to any surveillance. The question presented is whether the district court erred in nonetheless declining to dismiss the case, and instead calling for *in camera* proceedings that could risk the disclosure of state secrets.

STATEMENT OF THE CASE

Plaintiffs are Al-Haramain Islamic Foundation, Inc., an entity designated by the United States and the United Nations as a terrorist organization, and two lawyers affiliated with Al-Haramain. Plaintiffs alleged that they were subjected to warrantless foreign intelligence surveillance under the TSP, which the President authorized in the aftermath of the September 11, 2001 attacks to protect against future terrorist attacks. ER 501-08. The Government formally invoked the state secrets privilege and moved for dismissal or summary judgment because the very subject matter of this action is a state secret and the case cannot be litigated without recourse to highly classified state secrets concerning foreign intelligence gathering.

097

In response, the Government asserted the state secrets privilege and related statutory privileges, and moved for dismissal or summary judgment. See Motion to Dismiss Or, In the Alternative, For Summary Judgment (June 21, 2006). The state secrets privilege, which must be invoked by the pertinent agency head, requires dismissal whenever "there is a reasonable danger" that disclosing information in court proceedings would harm national security interests, such as by disclosing intelligence-gathering methods or capabilities. See *Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998). Dismissal is required if the action's "very subject matter" is a state secret, or if the plaintiff cannot prove a *prima facie* case, or the defendant cannot establish a valid defense, without information protected by the privilege. See *ibid.*

The Government's motion was supported by public and classified declarations of the then-Director of National Intelligence, John Negroponte, and the NSA's Director, General Keith Alexander. The Government also filed public and *ex parte/in camera* briefs, explaining that it could neither confirm nor deny whether plaintiffs had been surveilled under the TSP or any other intelligence-gathering program, and that litigation of plaintiffs' claims threatened disclosure of intelligence information, sources, and methods. See Mem. In Support of Motion (June 21, 2006).

[REDACTED TEXT—PUBLIC TEXT CONTINUES ON PAGE 7]

098

EXHIBIT U

Exh. 156
#2

KARIN J. IMMERGUT, OSB #963143
United States Attorney
District of Oregon
CHRISTOPHER L. CARDANI
Assistant United States Attorney
701 High Street
Eugene, OR 97401
(541) 465-6771
chris.cardani@usdoj.gov

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

UNITED STATES OF AMERICA,	)	No. CR 05-60008-01
Plaintiff,	)	GOVERNMENT'S MEMORANDUM IN SUPPORT OF PRETRIAL DETENTION
v.	)	
PEROUZ SEDAGHATY, a/k/a Pete Seda and Abu Yunus,	)	
Defendant.	)	

The United States of America, through its undersigned counsel, herein submits this memorandum in advance of defendant Sedaghaty's detention hearing, scheduled for Wednesday, August 22, 2007.

Despite defendant's voluntary return to the United States, the government believes that no set of conditions can be imposed upon defendant Sedaghaty that will reasonably assure the safety of the community and his appearance at trial. Support for this position is drawn from this memorandum, exhibits submitted with this memorandum, and from testimony anticipated at the detention hearing.

Your brothers, the Mujahideens (Ussamah Bin Laden Brigade).

Visit our site at www.laden.s5.com/ladenindex.htm

Although it is unknown who authored this message, it was dated October 10, 2001, which is three days after the United States began bombing Afghanistan after the terrorist attacks of 9-11. Testimony at the detention hearing will provide more context to this troubling e-mail.

The images and writings reviewed above, when considered in conjunction with the actions of defendant Sedaghaty, show that he not only ideologically agrees with the efforts of the *mujahideen*, but has supported them with funding and other types of logistical support from within the United States. Witting facilitation of radical Islamist fighters, and the distribution of hateful, violent literature to prisoners exhorting violence, makes defendant Sedaghaty a danger to the community.

Flight Risk

Defendant Sedaghaty departed the United States shortly after he was interviewed by the FBI in February 2003 and, so far as the government is aware, he did not return to the United States until four and a half years later, on August 15, 2007. While away from the United States, he retained a criminal defense attorney in Oregon to represent him during the criminal investigation. This attorney met with criminal investigators and the prosecutor both prior to and after defendant Sedaghaty was indicted.

Events significant to the timeline of defendant's absence from this country include:

February 2003 - Sedaghaty interviewed by the FBI and departs shortly

		thereafter
February 2004	-	Law enforcement execute search warrant at AHIF-US building in Ashland, Oregon
February 2004	-	OFAC issued a preliminary designation of AHIF-US as an SDGT (public notice provided)
June 2004	-	The Kingdom of Saudi Arabia dissolved AHIF-SA.
September 2004	-	OFAC and the UN issue a formal designation of AHIF-US and defendant Al-Buthe as terrorist supporters
February 2005	-	AHIF-US and defendants Sedaghaty and Al-Buthe indicted by a federal grand jury in Eugene, Oregon. This Court issues arrest warrants.
August 15, 2007	-	Defendant Sedaghaty is arrested at the Portland, Oregon International Airport after voluntarily returning to the United States.

Defendant Sedaghaty's criminal defense attorney met with defendant Sedaghaty outside the United States while he was a fugitive.[8] Defendant Sedaghaty has known that he was indicted and the subject of an arrest warrant for at least two and a half years.[9]

---

[8]To be clear, Sedaghaty was not a fugitive when he left the United States in 2003; he became a fugitive by operation of law when he was indicted in 2005, and the arrest warrant was issued, which defendant Sedaghaty had knowledge of while abroad.

[9]Exhibit P is an Associated Press article appearing on February 20, 2005, and states in part: "Lynne Bernabei, the Washington, D.C. lawyer representing Seda, Al-Buthe and Al-Haramain's Ashland chapter in the terrorist designation case, told the (Medford) Mail-Tribune that Seda is familiar with the charges against him and will return

EXHIBIT V

Statement
United States Senate Committee on the Judiciary
FISA for the 21st Century
July 26, 2006

General Michael V. Hayden
Director of Central Intelligence , Central Intelligence Agency

Testimony to the Judiciary Committee of the US Senate
By General Michael V. Hayden,
Director, CIA

26 July 2006

Mister Chairman, Senator Leahy, thank you for the opportunity to speak before your committee today. The work that you and we have before us is truly important: how dowe best balance our security and our liberty in the pursuit of legitimate foreign intelligence. Let me congratulate the Committee for taking on the task of examining and--where appropriate--amending the Foreign Intelligence Surveillance Act.

This task of balancing liberty and security is one that those of us in the intelligence community take very seriously and one to which we constantly turn our attention.

I recall that within days of the 9-11 attacks I addressed the NSA workforce to lay out our mission in a new environment. It was a short video talk beamed throughout our headquarters at Fort Meade and globally. Most of what I said was what anyone would expect. I tried to inspire. Our work was important and the Nation was relying on us. I tried to comfort. Look on the bright side: right now a quarter billion Americans wished they had your job. I ended the talk by trying to give perspective. All free peoples have had to balance the demands of liberty with the demands of security. Historically we Americans had planted our flag well down the spectrum toward liberty. Here was our challenge. "We were going to keep America free," I said, "by making Americans feel safe again."

This was not an easy challenge. The Joint Inquiry Commission (comprised of the House and Senate Intelligence Committees) would summarize our shortcomings in the months and years leading to the September 11th attacks. The Commission harshly criticized our ability to link things happening in the United States with things that were happening elsewhere.

Let me note some of JIC's Systemic Findings (Joint HPSCI-SSCI, from abridged findings and conclusions)

"...NSA's cautious approach to any collection of intelligence relating to activities in the United

States" (finding 7)

"There were also gaps in NSA's coverage of foreign communications and the FBI's coverage of domestic communications" (Finding 1, p 36, tab 4)

"...NSA did not want to be perceived as targeting individuals in the United States." (Finding 1, p 36, tab 4)

"[in talking about one end US conversations]...there was insufficient focus on what many would have thought was among the most critically important kinds of terrorist related communications, at least in terms of protecting the homeland." (Finding 1, p. 36, tab 4)

For NSA the challenge was especially acute. NSA intercepts communications and it does so for only one purpose: to protect the lives, the liberties and the well being of the citizens of the United States from those who would do us harm. By the late 1990s, that job was becoming very difficult. The explosion of modern communications in terms of its volume, variety and velocity threatened to overwhelm the Agency.

The September 11th attacks exposed an even more critical fault line. The laws of the United States do (and should) distinguish between the information space that is America and the rest of the planet.

But modern telecommunications do not so cleanly respect that geographic distinction. We exist on a unitary, integrated, global telecommunications grid in which geography is an increasingly irrelevant factor. What does "place" mean when one is traversing the World Wide Web? There are no area codes on the Internet.

And if modern telecommunications muted the distinctions of geography, our enemy seemed to want to end the distinction altogether. After all, he killed 3000 of our countrymen from within the homeland.

In terms of both technology and the character of our enemy, "in" America and "of" America no longer were synonymous.

I testified about this challenge in open session to the House Intelligence Committee in April of the year 2000. At the time I created some looks of disbelief when I said that if Usama bin Ladin crossed the bridge from Niagara Falls, Ontario to Niagara Falls, New York, there were provisions of US law that would kick in, offer him some protections and affect how NSA could now cover him. At the time I was just using this as a stark hypothetical. Seventeen months later this was about life and death.

The legal regime under which NSA was operating--the Foreign Intelligence Surveillance Act--had been crafted to protect American liberty and American security.

But the revolution in telecommunications technology has extended the actual impact of the FISA regime far beyond what Congress could ever have anticipated in 1978. And I don't think that anyone could make the claim that the FISA statute was optimized to deal with a 9/11 or to deal with a lethal enemy who likely already had combatants inside the United States.

Because of the wording of the statute, the government looks to four factors in assessing whether or not a court order was required before NSA can lawfully intercept a communication: who was the target, where was the target, how did we intercept the communication, and where did we intercept the

communication.

The bill before the committee today effectively re-examines the relevance of each of these factors and the criteria we want to use with each.

Who is the target?

The FISA regime from 1978 onward focused on specific court orders, against individual targets, individually justified and individually documented. This was well suited to stable, foreign entities on which we wanted to focus for extended period of time for foreign intelligence purposes. It is less well suited to provide the agility to detect and prevent attacks against the homeland.

In short, its careful, individualized processes exacted little cost when the goal was long term and exhaustive intelligence coverage against a known and recognizable agent of a foreign power. The costs were different when the objective was to detect and prevent attacks, when we are in hot pursuit of communications entering or leaving the United States involving someone associated with al Qa'ida.

In this regard, extending the period for emergency FISA's to seven days and allowing the Attorney General to delegate his authority to grant emergency orders is also very welcome and appropriate.

Where is the target?

As I said earlier, geography is becoming less relevant. In the age of the Internet and a global communications grid that routes communications by the cheapest available bandwidth available each nanosecond, should our statutes presume that all communications that touch America should be equally protected?

As the Chairman noted earlier this week, we do not limit our liberties by exempting from FISA's jurisdiction communications between two persons overseas that gets routed through US facilities.

Our limited government resources should focus on protecting US persons, not those entities who get covered as a result of technological changes that extend the impact--and protection--of FISA far beyond what its drafters intended.

I know that Senator DeWine among others has been very concerned about allocations of these resources and FISA backlogs. As Director of CIA I share his concerns in allocating my resources and hope that this legislation will help properly focus resources on protecting the legitimate privacy rights of US persons.

How did we intercept the communication?

For reasons that seemed sound at the time, current statute makes a distinction between collection "on a wire" and collection out of the air. When the law was passed, almost all local calls were on a wire and almost all long haul communications were in the air. In an age of cell phones and fiber optic cables, that has been reversed...with powerful and unintended consequences for how NSA can lawful acquire a signal. Legislators in1978 should not have been expected to predict the future of global telecommunications. Neither should you. The statute should be technology neutral.

Where we intercept the communication?

106

A single communication can transit the world even if the communicants are only a few miles apart. And in that transit NSA may have multiple opportunities to intercept it as it moves and changes medium. As long as a communication is otherwise lawfully targeted, we should be indifferent to where the intercept is achieved. Signals intelligence is a difficult art and science, especially in today's telecommunication universe. Intercept of a particular communication--one that would help protect the homeland, for example--is always probabilistic, not deterministic. No coverage is guaranteed. We need to be able to use all the technological tools we have.

In that light, there are no communications more important to the safety of the Homeland than those affiliated with al Qa'ida with one end in the United States. And so why should our laws make it more difficult to target the al Qa'ida communications that are most important to us--those entering or leaving the United States!

Because of the nature of global communications, we are playing with a tremendous home field advantage and we need to exploit this edge. We also need to protect this edge and those who provide it. The legislative language requiring compulsory compliance from carriers is an important step in this regard.

After 9/11, patriotic Americans assisted the Intelligence Community in ensuring that we have not had another attack on our soil since that awful day. And prior to 9/11, we received critical assistance across the IC from private entities. As Director of NSA, Deputy DNI, and now Director of the CIA, I understand that government cannot do everything. At times, we need assistance from outside the government.

Whatever legal differences and debates may occur about separation of powers, Article 2, and so on, those people who provide help to protect America should not suffer as a part of this debate. I would urge the committee to recognize the importance of the efforts of these Americans and provide appropriate protection.

One final--and very important--point. Many of the steps contained in the proposed legislation will address the issue raised by the Congress' Joint Inquiry Commission: one end US conversations, communications that the JIC characterized as "among the most critically important kinds of terrorist related communications, at least in terms of protecting the homeland."

That means NSA will bump up against information to, from or about US persons. Let me stress that NSA routinely deals with this challenge and knows how to do this while protecting US privacy. The draft bill contains quite a bit of language about minimization--the process NSA uses to protect US identities. The same rules of minimization that NSA uses globally, rules approved by the Attorney General and thoroughly briefed to Congress, will be used.

Let me close by saying that we have a great opportunity here today. We can meet the original intent of the FISA Act to protect our liberty and our security by making the legislation relevant to both the technologies and the enemies we face.

Thank you.

EXHIBIT W

HEARING OF THE SENATE SELECT COMMITTEE ON INTELLIGENCE
PROPOSED FISA MODERNIZATION LEGISLATION

WITNESSES:

MR. MIKE McCONNELL, DIRECTOR OF NATIONAL INTELLIGENCE;

LTG KEITH ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY;

MR. KENNETH WAINSTEIN, ASSISTANT ATTORNEY GENERAL FOR NATIONAL SECURITY, DEPARTMENT OF JUSTICE;

MR. BENJAMIN POWELL, GENERAL COUNSEL, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE;

MR. VITO POTENZA, GENERAL COUNSEL, NATIONAL SECURITY AGENCY

CHAIRED BY: SENATOR JOHN D. ROCKEFELLER IV (D-WV)

LOCATION: 106 DIRKSEN SENATE OFFICE BUILDING, WASHINGTON, D.C.

TIME: 2:30 P.M. EDT
DATE: TUESDAY, MAY 1, 2007

SEN. ROCKEFELLER: This hearing has begun, and I welcome all of our testifiers. And other members of the committee will be coming in. I know some of the caucuses just broke up.

The Select Committee on Intelligence meets today in open session, something we don't ought to do, to consider whether the scope and application regarding the Surveillance Act needs to changed to reflect the evolving needs for the timely collection of foreign intelligence. An extraordinarily complicated subject, this is. At the committee's request, the administration has undertaken a comprehensive review of the Foreign Intelligence Surveillance Act, commonly referred to as FISA. Out of this review, the administration proposed -- it believes would modernize the laws governing the way in which we gather foreign intelligence with the use of electronic surveillance.

Consideration of the administration's proposal and alternatives will be rooted in the Intelligence Committee's 30-year experience with our nation's long and delicate effort to strike that elusive right balance between effective intelligence collection for our national security and the constitutional rights and privacy interests of Americans.

The Intelligence Committee's existence came out of the work of the Church Committee and others in the mid-'70s to bring to light abuses in the electronic surveillance of Americans. One of the committee's first tasks was to work with the Senate Judiciary Committee and with the Ford and Carter administrations from 1976 to 1978 to enact the Foreign Intelligence Surveillance Act. As we take a fresh look at the current law, we will again be working with our colleagues in the Senate Judiciary Committee.

FISA involves both the judicial process on the one hand and the collection of intelligence. Our committee's contribution to this process

MR. MIKE McCONNELL: Good afternoon, Chairman Rockefeller, Vice Chairman Bond, members of the committee. Thank you for inviting us to come today to engage with the Congress on legislation that will modernize the Foreign Intelligence Surveillance Act, as you mentioned, FISA -- I'll refer to it as FISA from this point on -- which was passed in 1978.

In response to your guidance from last year on the need to revise FISA, the administration has worked for over the past year, with many of you and your staff experts, to craft the proposed legislative draft. It will help our intelligence professionals, if passed, protect the nation by preventing terrorist acts inside the United States. Since 1978, FISA has served as the foundation to conduct electronic surveillance of foreign powers or agents of foreign powers inside the United States. We are here today to share with you the criticality -- critical important role that FISA plays in protecting the nation's security, and how I believe the proposed legislation will improve that role, while continuing to protect the civil and the privacy rights of all Americans.

The proposed legislation to amend FISA has four key characteristics. First, it makes the statute technology-neutral. It seeks to bring FISA up to date with the changes in communications technology that have taken place since 1978. Second, it seeks to restore FISA to its original focus on protecting the privacy interests of persons inside the United States. Third, it enhances the government's authority to secure assistance by private entities, which is vital for the intelligence community to be successful. And fourth, it makes changes that will streamline FISA administrative processes so that the intelligence community can use FISA as a tool to gather foreign intelligence information more quickly and more effectively.

The four critical questions, four critical questions that we must address in collection against foreign powers or agents of foreign powers are the following. First, who is the target of the communications? Second, where is the target located? Third, how do we intercept the communications? And fourth, where do we intercept the communications? Where we intercept the communications has become a very important part of the determination that must be considered in updating FISA.

As the committee is aware, I've spent the majority of my professional life in or serving the intelligence community. In that capacity, I've been both a collector of information and a consumer of intelligence information. I had the honor of serving as the director of the National Security Agency from 1992 to 1996. In that position, I was fully aware of how FISA serves a critical function enabling the collection of foreign intelligence information.

In my first 10 weeks on the job as the new director of National Intelligence, I immediately can see the results of FISA-authorized collection activity. The threats faced by our nation, as I have previously testified to this committee, are very complex and there are very many. I cannot overstate how instrumental FISA has been in helping the intelligence community protect the nation from terrorist attacks since September 11th, 2001.

Some of the specifics that support my testimony, as has been mentioned, cannot be discussed in open session. This is because certain information about our capabilities could cause us to lose the capability if known to the terrorists. I look forward to elaborating further on aspects of the issues in a closed session that is scheduled to follow.

I can, however, make the following summary-level comment about the current FISA legislation. Since the law was drafted in a period preceding today's global information technology transformation and does not address today's global systems in today's terms, the intelligence community is significantly burdened in capturing overseas communications of foreign terrorists planning to conduct attacks inside the United States.

Let me repeat that for emphasis. We are significantly burdened in capturing overseas communications of foreign terrorists planning to conduct attacks inside the United States. We must make the requested changes to protect our citizens and the nation. In today's threat environment, the FISA legislation is not agile enough to handle the community's and the country's intelligence needs. Enacted nearly 30 years ago, it has not kept pace with 21st century developments in communications technology. As a result, FISA frequently requires judicial authorization to collect the communications of non-U.S. -- that is, foreign -- persons located outside the United States.

Let me repeat again for emphasis. As a result, today's FISA requires judicial authorization to collect communications of non-U.S. persons -- i.e., foreigners -- located outside the United States. This clogs the FISA process with matters that have little to do with protecting civil liberties or privacy of persons in the United States. Modernizing FISA would greatly improve that process and relieve the massive amounts of analytic resources currently being used to craft FISA applications.

FISA was enacted before cell phones, before e-mail and before the internet was a tool used by hundreds of millions of people worldwide every day.

There are two kinds of communications. It's important to just recapture the fact, two kinds of communications: wire and wireless. It's either on a wire -- could be a copper wire, a fiber wire -- it's on a wire or it's wireless, meaning it's transmitted through the atmosphere.

When the law was passed in 1978, almost all local calls were on a wire. Almost all local calls, meaning in the United States, were on a wire, and almost all long-haul communications were in the air, were known as wireless communications. Therefore, FISA in 1978 was written to distinguish between collection on a wire and collection out of the air or against wireless.

Now in the age of modern communications today, the situation is completely reversed. It's completely reversed. Most long-haul communications -- think overseas -- are on a wire -- think fiberoptic pipe. And local calls are in the air. Think of using your cell phone for mobile communications.

Communications technology has evolved in ways that have had unforeseen consequences under FISA, passed in 1978. Technological changes have brought within FISA's scope communications that we believe the 1978 Congress did not intend to be covered. In short, communications currently fall under FISA that were originally excluded from the act. And that is foreign-to-foreign communications by parties located overseas.

The solution is to make FISA technology-neutral. Just as the Congress in 1978 could not anticipate today's technology, we cannot know what technology may bring in the next thirty years. Our job is to make the country as safe as possible by providing the highest quality intelligence available. There is no reason to tie the nation's security to a snapshot of outdated technology.

Additionally, FISA places a premium on the location of the collection. Legislators in 1978 could not have been expected to predict an integrated global communications grid that makes geography an increasingly irrelevant factor. Today, a single communication can transit the world even if the two people communicating are only located a few miles apart. And yet simply because our law has not kept pace with technology, communications intended to be excluded from FISA are in fact included. There is no real consequence -- this has real consequence on the intelligence community working to protect the nation.

Today intelligence agencies may apply, with the approval of the attorney general and the certification of other high level officials, for court orders to collect foreign intelligence information under FISA. Under the existing FISA statute, the intelligence community is often required to make a showing of probable cause.

Frequently, although not always, that person's communications are with another foreign person overseas. In such cases, the statutory requirement is to obtain a court order, based on a showing of probable cause, that slows, and in some cases prevents altogether, the government's effort to conduct surveillance of communications it believes are significant to national security, such as a terrorist coordinating attacks against the nation located overseas.

This is a point worth emphasizing, because I think many Americans would be surprised at what the current law requires. To state the case plainly: when seeking to monitor foreign persons suspected of involvement in terrorist activity who are physically located in foreign countries, the intelligence community is required under today's FISA to obtain a court order to conduct surveillance. We find ourselves in a position, because of the language in the 1978 FISA statute, simply -- we have not kept pace with the revolution in communications technology that allows the flexibility we need.

As stated earlier, this committee and the American people should know that the information we are seeking is foreign intelligence information. Specifically, this includes information relating to the capabilities, intentions and activities of foreign powers or agents of foreign powers, including information on international terrorist activities. FISA was intended to permit the surveillance of foreign intelligence targets while providing appropriate protection through court supervision to U.S. citizens and other persons located inside the United States.

Debates concerning the extent of the president's constitutional powers were heated in the mid-'70s, as indeed they are today. We believe that the judgment of the Congress at that time was that the FISA regime of court supervision was focused on situations where Fourth Amendment interests of persons in the United States were implicated. Nothing -- and I would repeat -- nothing in the proposed legislation changes this basic premise in the law.

complete understanding of how the statute has been interpreted and how it's being currently used. I don't know how you legislate that way. MR. WAINSTEIN: Well, I understand, but obviously, every time they issue an order, that is -- that can be an interpretation of how the FISA statute is -- interpretation of the FISA statute. And as you know from the numbers that we issue, we have a couple thousand FISAs a year. So that would be quite a few documents.

SEN. FEINGOLD: This is an important matter. If that's the number of items we need to look at, that's the number we will look at.

Thank you, Mr. Chairman.

SEN. ROCKEFELLER: Thank you, Senator Feingold.

Senator Nelson.

SEN. BILL NELSON (D-FL): Mr. Chairman, most of my questions I'm going to save for the closed session, but I would like to ascertain the administration's state of mind with regard to the current law. In the case where there is a foreign national in a foreign land calling into the United States, if you do not know the recipient's nationality and therefore it is possible it is a U.S. citizen, do you have to, in your interpretation of the current law, go and get a FISA order?

MR. McCONNELL: No, sir, not if it -- if the target is in a foreign country and our objective is to collect against the foreign target, and they call into the United States, currently it would not require a FISA. And let me double-check that. I may be -- I'm dated.

LTG ALEXANDER: If it's collected in the United States, it would require a FISA if we do not know who the end is to, or under the program it would have to be collected. If it were known, both ends foreign, known a priori, which is hard to do in this case, you would not. If it was collected overseas, you would not.

SEN. BILL NELSON: Let's go back to your second -- General, your second answer.

LTG ALEXANDER: If you know both ends -- where the call is going to go to before he makes the call, then you know that both ends were foreign; if you knew that ahead of time, you would not need a warrant.

SEN. NELSON: If you knew that.

LTG ALEXANDER: If you knew that.

SEN. NELSON: If you did not know that the recipient of the call in the U.S. is foreign, then you would have to have a FISA order.

LTG ALEXANDER: If you collected it in the United States. If you collected it overseas, you would not.

SEN. NELSON: Well, since in digital communications, if these things -- little packets of information are going all over the globe, you might be collecting it outside the United States, you might be collecting it inside the United States.

MR. McCONNELL: And Senator, that's our dilemma. In the time in 1978 when it was passed, almost everything in the United States was wire, and it was called electronic surveillance. Everything external in the United States was in the air, and it was called communications intelligence.

So what changed is now things in the United States are in the air, and things outside are on wire. That's the --

SEN. NELSON: I understand that, but -- now, I got two different answers to the same question from you, Mr. Director, and from you, General.

MR. McCONNELL: It depends on where the target is and where you collect it. That's why you heard different answers.

SEN. NELSON: So if you're collecting the information in the United States --

MR. McCONNELL: It requires a FISA.

SEN. NELSON: Okay. Under the current law, the president is allowed 72 hours in which he can go ahead and collect information and, after the fact, go back and get the FISA order.

Why was that suspended before in the collection of information?

LTG ALEXANDER: Sir, I think that would best be answered in closed session to give you exactly the correct answer, and I think I can do that.

SEN. NELSON: And -- well, then, you can acknowledge here that is -- it was in fact suspended.

SEN. ROCKEFELLER: I would hope that that would be -- we would leave this where it is.

SEN. NELSON: All right. I'll just stop there.

SEN. ROCKEFELLER: Thank you, Senator Nelson.

Senator Feinstein.

SEN. DIANNE FEINSTEIN (D-CA): Thank you very much, Mr. Chairman. The administration's proposal, Admiral, doesn't address the authority that the president and attorney general have claimed in conducting electronic surveillance outside of FISA. While the FISA Court issued a ruling that authorized the surveillance ongoing under the so-called TSP, Terrorist Surveillance Program, the White House has never acknowledged that it needs court approval. In fact, the president, under this reasoning, could restart the TSP tomorrow without court supervision if he so desired.

Now, Senator Specter and I have introduced legislation which very clearly establishes that FISA is the exclusive authority for conducting intelligence in the United States.

Here's the question: Does the administration still believe that it has the inherent authority to conduct electronic surveillance of the type done under the TSP without a warrant?

EXHIBIT X

HEARING OF THE HOUSE SELECT INTELLIGENCE COMMITTEE
(Embedded image moved to file: pic21722.gif)SUBJECT: THE FOREIGN INTELLIGENCE SURVEILLANCE ACT
(Embedded image moved to file: pic23958.gif)CHAIRED BY: REP. SILVESTRE REYES (D-TX)
(Embedded image moved to file: pic18429.gif)WITNESSES: DIRECTOR OF NATIONAL INTELLIGENCE MIKE MCCONNELL; KENNETH WAINSTEIN, ASSISTANT ATTORNEY GENERAL
IN THE DEPARTMENT OF JUSTICE'S NATIONAL SECURITY DIVISION

1300 LONGWORTH HOUSE OFFICE BUILDING, WASHINGTON, D.C.
9:14 A.M. EDT, THURSDAY, SEPTEMBER 20, 2007

REP. REYES: (Sounds gavel.) The committee will please come to order. Today the committee will receive testimony from the director of national intelligence, Admiral Michael McConnell, and the assistant attorney general for national security, Mr. Kenneth Wainstein, who is -- who we're waiting on now -- concerning the Foreign Intelligence Surveillance Act, and the recently enacted legislation that expanded the administration's surveillance powers; the Protect America Act, or as commonly referred to, the PAA.

REP. REYES: I want to thank my colleague from California for clarifying the fact that we may be spying on our soldiers.

With that, Director McConnell, you are recognized for your opening statement.

ADM. MCCONNELL: Thank you, Senator, ranking member Hoekstra, members of the committee, a pleasure to appear before you today.

I appreciate the opportunity to discuss the Protect America Act-- I will refer to it as PAA -- and the need for lasting modernization of the Foreign Intelligence Surveillance Act of course we'll refer to as the FISA.

I'm pleased to be joined today by Assistant Attorney General Ken Wainstein of the Department of Justice national security division.

It is my belief that the first responsibility of intelligence is to achieve understanding and to provide warning. AS the head of the nation's intelligence community, it is not only my desire but in fact my duty to encourage changes to policies and procedures, and where needed, legislation to improve our ability to provide warning of terrorist or other attacks to the country.

On taking up this post it became clear to me that our foreign intelligence capabilities were being degraded. I learned that collection using authorities provided by FISA continued to be instrumental in protecting the nation, but due to changes in technology, the law was actually preventing us from collecting foreign intelligence.

I learned that members of Congress in both chambers, and on both sides of the aisle had in fact proposed legislation to modernize FISA, and this was accomplished in 2006. In fact a bill was passed in the House in 2006.

And so the dialog on FISA has been ongoing for some time. This has been a constructive dialog, and I hope it continues in the furtherance of serving the nation to protect our citizens.

None of us want a repeat of the 9/11 attacks, although al Qaeda has stated their intention to conduct another such attack.

When the law was passed in '78 almost all local calls in the United States were on a wire, and almost all international calls were in the air, known as wireless. Therefore FISA was written in 1978 to distinguish between collection on wire and collection out of the air.

Today the ~~situation is completely~~ reversed. Most international communications are on a wire, ~~fiber optic cable, and local calls are in the air. FISA was originally~~ -- FISA also originally placed a premium on the location of the collection. ~~There was the cause of our problem,~~ on a wire, in the United States, equal a warrant requirement even if it was against a foreign person located overseas.

Because of these changes in technology communications intended to be excluded from FISA in 1978 were in fact frequently included in 2007. This had real consequences. It meant the community in a significant number of cases was required to demonstrate probable cause to a court to collect communications of a foreign intelligence target located overseas. And that's very important, and I would emphasize it. Probable cause level of justification to collect against a foreign target located overseas.

Because of this, the old FISA's requirements prevented the intelligence community from collecting important intelligence information on current threats.

In a debate over the summer, and since, I've heard individuals both inside the government and outside assert that the threats to our nation do not justify this authority. Indeed, I've been accused of exaggerating the threat that the nation faces. Allow me to attempt to dispel that notion.

The threats that we face are real, and they are serious. In July of this year we released the National Intelligence Estimate, we refer to it as the NIE, on the terrorist threat to the homeland. The NIE is the community's most authoritative written judgment on a particular subject. It is coordinated among all 16 agencies of the community.

The key judgments from this NIE are posted on a website, and I would encourage all to review the full details.

In short the NIE's assessments stated the following. The U.S. homeland will face a persistent and evolving terrorist threat over the next three years. That's the period of the estimate. The main threats come from Islamic terrorist groups and cells, and most especially al Qaeda.

values. There are three key areas that continue to need attention. For reasons that I've outlined today, it's critical that the FISA's definition of electronic surveillance be amended permanently so that it does not cover foreign intelligence targets reasonably believed to be located outside the United States. Second, I call on Congress to act swiftly to provide retroactive liability protection to the private sector. It is important to keep in mind that the intelligence community often needs the assistance of the private sector to protect the nation. We simply cannot go alone. We must provide protection to the private sector so that they can assist the community in protecting the nation while adhering to their own corporate fiduciary duties. Thirdly, in April 2007 in the bill that we submitted to Congress, we asked for a number of streamlined provisions that would make processing FISA applications more effective and efficient. These changes would substantially improve the FISA process without affecting the important substantive requirements of the law. Finally, we understand and fully support the requirement for the community to obtain a court order or a warrant any time the target for foreign surveillance is located inside the United States. That was true in 1978 when the law was originally passed. It is true today with the update that became law last month.

Mr. Chairman, that completes my remarks. I'd be happy to answer your questions.

REP. REYES: Thank you, Admiral.

With that, we recognize Mr. Wainstein for his opening statement.

MR. WAINSTEIN: Chairman Reyes, Ranking Member Hoekstra and members of the committee, good morning and thank you very much for this opportunity to testify before you again concerning FISA modernization. I'm proud to be here to represent the Department of Justice, and I'm happy to discuss this important issue with you.

The Protect America Act is an important law that has allowed the intelligence community to close intelligence gaps caused by FISA's outdated provisions, and it has already made a difference, it has already made our nation safer. In my statement this afternoon, I'll briefly explain why I believe Congress should make the Protect America Act permanent and also enact other important reforms to the FISA statute. But before I do that, I would like to thank this committee for having me in closed session last week.

And in particular, I'd like to thank you, Chairman Reyes, for proposing that we send you a letter laying out our position on some of the concerns that you and other members of the committee had with certain parts

of the Protect America Act, concerns that certain language might permit the government to conduct intelligence activities well beyond those that Congress contemplated when it passed the statute. As the committee is aware, we drafted and sent you that letter last Friday, and it laid out why it is that we don't think those concerns will become a reality in practice. I appreciated the opportunity to engage in that dialogue with you and your colleagues, Chairman Reyes, and I look forward to continuing it here today. I believe that this process will help to reassure Congress and the American people that the act you passed in August is a measured and sound approach to a critically important issue facing our nation.

Let me turn briefly now to why I believe the act should be made permanent. As I explained in my prior testimony, in 1978, Congress designed a judicial review process that applied primarily to surveillance activities within the United States where privacy interests are the most pronounced and not to overseas surveillance against foreign targets where (cognoscible ?) privacy interests are minimal or nonexistent. They did this very much intentionally as they were working against a constitutional backdrop articulated in case law and in legislation that did not extend 4th Amendment protections to foreigners overseas and that left the conduct of foreign intelligence surveillance against foreigners overseas within the ambit and authority of the executive branch.

With this historical backdrop in mind, Congress created a dichotomy in the statute, a dichotomy between domestic surveillance that is governed by FISA, and is therefore subject to FISA court review and approval, and overseas surveillance against foreign targets that is not. Congress established this dichotomy by distinguishing between wire communications which included most of the local and domestic traffic in 1978 and which were largely brought within the scope of the statute and radio communications which included most of the transoceanic traffic of the time and were largely left outside the scope of the statute.

As a result of the revolutions in telecommunications technology over the last 29 years, much of the international communications traffic is now conducted over fiber optic cables which qualify as wire communications under the statute. As a result, many of the surveillances directed at persons overseas which were not intended to fall within FISA became subject to FISA requiring us to seek court authorization before initiating surveillance and effectively conferring quasi-constitutional protections on terrorist suspects overseas. This process impaired our surveillance efforts and diverted resources that were better spent protecting the privacy interests of Americans here in America.

As the committee is aware, the administration had submitted to Congress a comprehensive proposal in April that would remedy this problem and provide a number of other refinements and important changes to the FISA

120

EXHIBIT Y

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

AMERICAN CIVIL LIBERTIES UNION; AMERICAN CIVIL LIBERTIES UNION FOUNDATION; AMERICAN CIVIL LIBERTIES UNION OF MICHIGAN; COUNCIL ON AMERICAN-ISLAMIC RELATIONS; COUNCIL ON AMERICAN-ISLAMIC RELATIONS MICHIGAN; GREENPEACE, INC.; NATIONAL ASSOC. OF CRIMINAL DEFENSE LAWYERS; JAMES BAMFORD; LARRY DIAMOND; CHRISTOPHER HITCHENS; TARA MCKELVEY; and BARNETT R. RUBIN,
Plaintiffs,

v.

CIVIL ACTION
NO. 06-10204

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE; and LIEUTENANT GENERAL KEITH B. ALEXANDER, in his official capacity as Director of the National Security Agency and Chief of the Central Security Service,
Defendants.
_____/

MOTION FOR PARTIAL SUMMARY JUDGMENT
BEFORE THE HONORABLE ANNA DIGGS TAYLOR
United States District Judge
231 Lafayette Boulevard West
Detroit, Michigan
Monday, June 12, 2006

APPEARANCES:

American Civil Liberties Union Foundation
MS. ANN BEESON
125 Broad Street-18th Floor
New York, New York 10004
(212) 549-2601
On behalf of Plaintiffs.

United States Department of Justice
ANTHONY J. COPPOLINO
20 Massachusetts Avenue, N.W.
Washington, D.C. 20530
(202) 514-4782
On behalf of Defendants.

TO OBTAIN CERTIFIED TRANSCRIPT:
Andrea E. Wabeke, CSR, RMR, CRR
734.741.2106 x1144

monitoring. And as a result of that actual action by the Government against those targets, the court said, well, there was a decrease in attendance at church and people were concerned but it was not speculation, it was something the Government did.

Here, their claims of standing are based on allegations that we're actually surveilling them and those are just based on an assumption that is not founded in fact. It sounds like, and I haven't read this case because she didn't cite it in her brief, it sounds like the Socialist Workers Party case is the same thing. The Government attended the meeting or threatened to attend the meeting, and therefore it was an actual injury to those who were there.

The point I'm trying to make, your Honor, is that if you want to get standing based on an allegation of subjective chill, the Government must actually do something to you and that must be clear. You don't have standing just by saying a program exists, we're modifying our behavior because we think it might cover us, and that's what their claims are, and it's not sufficient.

Now, let me address more specifically the argument that those attorneys who would represent terrorist clients have standing. I certainly

recognize that in that respect, those plaintiffs come closer to being in the ballpark with the terrorist surveillance program, as opposed to the plaintiffs who say I'm inhibited from talking to my families in the Middle East and Asia, as if that somehow everybody in the Middle East and Asia is related to Al Qaeda, or I can't talk about political topics, or I can't talk about the war or I can't talk about human rights in China. Those folks are out of the box completely. Those attorneys who say, however, I represent Al Qaeda, they seem closer to being within the framework of the terrorist surveillance program.

But a couple points about that, your Honor. One is, as the court in United Presbyterian pointed out in the D.C. Circuit case, claims by a plaintiff that they're more likely for some reason to be subject to surveillance based on their activities is not enough. It may indeed be the case that plaintiffs who represent terrorist suspects are more likely to be subject to the program, but that doesn't adequately establish standing because it still doesn't show that they've actually been subject to any surveillance.

Judge Scalia wrote: That kind of allegation does not adequately aver that the specific action is threatened or even contemplated against them. And so

EXHIBIT Z

TOP SECRET [redacted]

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

FAC No. SDG-392566

[redacted]

Date: February 6, 2008

MEMORANDUM FOR **ADAM J. SZUBIN**
DIRECTOR
OFFICE OF FOREIGN ASSETS CONTROL

FROM: Howard Mendelsohn /s/ 2/6/08
Deputy Assistant Secretary, Office of Intelligence and Analysis

SUBJECT: (U) Redesignation of Al-Haramain Islamic Foundation locations in the United States (**AHF-OREGON**), and AHF official **Soliman AL-BUTHE** pursuant to E.O. 13224

(U) INTRODUCTION

(U) President Bush issued Executive Order 13224 (E.O.) on September 23, 2001 declaring a national emergency to address grave acts of terrorism and threats of terrorism committed by foreign terrorists, including the September 11, 2001 terrorist attacks in New York, Pennsylvania, and the Pentagon. The E.O. authorizes the Secretary of the Treasury, in consultation with the Secretaries of State and Homeland Security,[1] and the Attorney General, to designate those persons determined to be:

(1) owned or controlled by, or to act for or on behalf of those persons listed in the Annex to the E.O., or those determined to be subject to subsection 1(b), 1(c), or 1(d)(i) of the E.O.;
(2) assisting in, sponsoring, or providing financial, material, or technological support for, or financial or other services to or in support of, such acts of terrorism or those persons listed in the Annex to E.O. 13224 or determined to be subject to the E.O.; or
(3) associated with those persons listed in the Annex, or those persons determined to be subject to subsection 1(b),1(c), or 1(d)(i) of the E.O.

(U) The following evidence in the files of the Office of Foreign Assets Control (OFAC) provides reason to believe that the entity and individual named below satisfy the criteria for designation pursuant to Executive Order 13224, "Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten to Commit, or Support Terrorism."

(U) [Note: The name of the individual and entity proposed for redesignation in this memorandum will appear throughout the following text in **BOLD CAPITAL** font, while the names of persons previously designated as Specially Designated Global Terrorists (SDGT) pursuant to E.O. 13224 will appear in **Bold Title** font.]

[redacted]
Derived from: Multiple Sources
Declassify on: [redacted]

[1] (U) E.O. 13224 was amended by E.O. 13284 (January 23, 2003) adding the Secretary of Homeland Security to the consultative process.

Redacted and released for Case # 07-CV-1155-KI U.S. District Court for the District of Oregon on 3/3/08

[redacted]

(U) Soliman AL-BUTHE

(U) AL-BUTHE has been identified as the Treasurer of AHF-OREGON, according to the U.S. AHF-OREGON tax form 990 for 2001 filed with the IRS. [Source: AHF-OREGON Tax Form 990, 2001, Exhibit 39] Resident in Riyadh, Saudi Arabia, AL-BUTHE also reportedly assisted in the establishment of AHF-OREGON, and served as the chairman of AHF's U.S. Committee, according to an Affidavit in Support of an Application for Search Warrant and local news reports. [Source: United States District Court, District of Oregon, Affidavit in Support of an Application for search Warrant, Exhibit 95; The Oregonian, January 10, 2004, Exhibit 121; The Sunday Oregonian, November 9, 2003, Exhibit 103] In a document signed by AHF's leader Al-Aqil, AHF in Saudi Arabia appointed AL-BUTHE "true and lawful attorney in [AHF's] name, place and stead," apparently giving AL-BUTHE broad legal authority to act on AHF's behalf in the U.S. [United States District Court, District of Oregon, Affidavit in Support of an Application for Search Warrant, Exhibit 95]

(S [redacted]

[Source: Knight Ridder/Tribune News Service, June 3, 2003, Exhibit 123; [redacted] AL-BUTHE's role as a senior AHF official is corroborated in part by information obtained by the FBI. A letter drafted on AHF "head office-Riyadh" stationery identifies AL-BUTHE as the President of AHF's Internet Committee. [Source: Copy of Government Exhibit F139a, Exhibit 127]

(U) Other evidence shows that AL-BUTHE had signature authority to sign contracts on behalf of AHF's head office in Riyadh, Saudi Arabia. On or about February 15, 2002, a "Memorandum of Agreement" showed that AL-BUTHE represented AHF in an agreement that was signed with a U.S. party for the development and distribution of religious materials. [Source: Government Exhibit F67A, Exhibit 128] In two other related contracts, AL-BUTHE also represented AHF in signing agreements. [Source: Copy of Government Exhibit F61A, Exhibit 129; E010(4B36-31-098 to 100), Exhibit 130]

[redacted]

(U) On February 18, 2004, Federal law enforcement authorities executed a search warrant against property purchased on behalf of AHF-OREGON. The search was conducted pursuant to

a criminal investigation into possible violations by AL-BUTHE (and Seda) of the Internal Revenue Code, the Money Laundering Control Act and the Bank Secrecy Act. In a separate administrative action, OFAC blocked pending investigation AHF accounts and real property in the U.S. to ensure the preservation of AHF assets pending further investigation. [Source: U.S. Department of Treasury, Press Room, February 19, 2004, Exhibit 94; United States District Court, District of Oregon, Affidavit in Support of an Application for Search Warrant, Exhibit 95]

[redacted]

(U) Additional Information on Soliman AL-BUTHE

[redacted]

(U//FOUO) AL-BUTHE and Seda were involved with the withdrawal of funds from the AHF-OREGON branch office bank account during March 2000. The withdrawn funds included a $150,000 contribution from Dr. Mahmoud Talaat El-Fiki. In a February 20, 2000 email to "haramain" notifying the organization of Fiki's contribution it was indicated that the money was given "as Zakat in order to participate in your noble support to our muslim brothers in Chychnia."[39] Also noted in the email was "our previous correspondence," and the fact that a request was made to Fiki's bank in London "to make a transaction to your USA account, *using*

[redacted]

the details you provided in an earlier email...," (emphasis added). The money subsequently was transported by **AL-BUTHE** to Saudi Arabia, at which point it is believed to have been sent to mujahideen in Chechnya. [Source: Pretrial Detention Request, Exhibit 156; Accompanying exhibit L of the Pretrial Detention Request, Exhibit 210]

(U) In support of the request for reconsideration of the designation of **AL-BUTHE**, **AL-BUTHE** counsel informed OFAC via correspondence that **AL-BUTHE** first learned of Fiki's contribution during early March 2000 – this despite the February 20, 2000 Fiki-related email which referenced "previous correspondence" and "details...provided in an earlier email." [Source: Correspondence from **AL-BUTHE** attorney Thomas Nelson to OFAC, January 19, 2005, Exhibit 154; accompanying exhibit L of the Pretrial Detention Request, Exhibit 210] The attorney correspondence also indicated that "**AL-BUTHE** is uncertain why Dr. Fiki (whom Mr. **AL-BUTHE** has never met) sent the contribution to the United States instead of Saudi Arabia," but **AL-BUTHE** "speculates that there probably are fewer restrictions on [affecting] such transfers into the United States." **AL-BUTHE** also speculated that Fiki may have responded to "website instructions or advertisements that had been published in Islamic magazines directing contributions to the United States." That speculation, however, appears inconsistent with the aforementioned reference to "previous correspondence" and with the fact that Fiki's contribution to the U.S. bank account was completed "using details...provided in an earlier email." [Source: Correspondence from **AL-BUTHE** attorney Thomas Nelson to OFAC, January 19, 2005, Exhibit 154; accompanying exhibit L from the Pretrial Detention Request, Exhibit 210]

(TS [redacted] In support of the request for reconsideration of the designation of **AL-BUTHE**, **AL-BUTHE** counsel also informed OFAC via correspondence that **AL-BUTHE** worked on the Saudi-based AHF website as early as 1993, and continued in this work as late as March 2000. Moreover, the letter indicated that the very purpose of **AL-BUTHE's** trip to the United States during March 2000 was to assist "in establishing an Islamic website, IslamToday."[40] Additionally, it is elaborated in the correspondence that **AL-BUTHE's** role with the AHF evolved over time to the point at which he became "responsible for internet activities and then for charitable works in the United States."[41] [Source: Correspondence from **AL-BUTHE** attorney Thomas Nelson to OFAC, January 19, 2005, Exhibit 154] According to the indictment of Seda and **AL-BUTHE**, the AHF website (www.alharamain.org), as of 1999 and 2000, contained numerous articles supportive of the Chechen mujahideen, to include reports such as "The Latest News About Jihaad in Chechnya." The website also contained a prayer for Chechen mujahideen, referring to them as the "Mujahideen brothers in Chechnya." The indictment further indicates that a link was provided via the AHF website to www.qoqaz.com, through which details could be obtained on how to fund Chechen mujahideen.[42] [Source: Copy

[40] (U) The March 2000 trip referenced here is the same trip during which Fiki's $150,000 contribution was withdrawn from the **AHF-OREGON** account and transported by **AL-BUTHE** from the United States to Saudi Arabia. [Source: Correspondence from **AL-BUTHE** attorney Thomas Nelson to OFAC, January 19, 2005, Exhibit 154]

[redacted]

of Indictment in U.S. v. AL-HARAMAIN ISLAMIC FOUNDATION, INC.; Pirouz SEDAGHATY, a/k/a Pete Seda, Perouz Seda Ghaty and Abu Yunus; and Soliman Hamd AL-BUTHE, Exhibit 165] Thus, an argument that AL-BUTHE was ignorant of AHF facilitation (e.g. via qoqaz.com) of funding of the Chechen mujahideen would be questionable given his internet-related responsibilities, his overt acts (transporting the $150,000 Fiki contribution), his official position with the AHF and its Oregon branch (supportive of Chechen mujahideen). [redacted] [Source: Correspondence from AL-BUTHE attorney Thomas Nelson to OFAC, January 19, 2005, Exhibit 154; letter presumably from AL-BUTHE identifying him as the President of the "Internet Committee" of AHF-Riyadh, Exhibit 127; copy of Indictment in U.S. v. AL-HARAMAIN ISLAMIC FOUNDATION, INC.; Pirouz SEDAGHATY, a/k/a Pete Seda, Perouz Seda Ghaty and Abu Yunus; and Soliman Hamd AL-BUTHE, Exhibit 165; [redacted]

[redacted]

Intercepts disclosed during Al-Timimi's trial (Al-Timimi was [redacted]

convicted and sentenced to life in prison) reveal a relationship between Al-Timimi and AL-BUTHE. AL-BUTHE was intercepted in some four conversations with Al-Timimi. In an intercept on February 1, 2003, at 15:38 Al-Timimi spoke with FNU LNU,[46] (subsequently determined to be **Soliman AL-BUTHE**). [Source: Copy of United States of America v. Ali Al-Timimi, United States District Court for the Eastern District of Virginia, Exhibit 168; Stipulations 17-24, United States District Court for the Eastern District of Virginia, Exhibit 204] During the conversation, FNU LNU provided Al-Timimi with the following fax number: 966-12066331. During the same intercept, FNU LNU passed the telephone to Ahmad LNU. After a brief conversation, Al-Timimi told Ahmad LNU to ask "Sulayman," (likely **Soliman AL-BUTHE**) to call him (Al-Timimi) the next day so that Al-Timimi could dictate something to "Sulayman." That same day at 16:20 Al-Timimi again was intercepted speaking to FNU LNU (subsequently determined to be **Soliman AL-BUTHE**). [Source: GX 10B4A, Copy of Ali Al-Timimi Telephone Intercept Linesheet, Exhibit 206; Stipulations 17-24, United States District Court for the Eastern District of Virginia, Exhibit 204] During the conversation FNU LNU provided Al-Timimi with the following U.S. telephone (probable fax) number: 253-981-9150. An internet query links both aforementioned telephone numbers with ICSFP.com and sb@whymuhammad.net. The latter internet addresses, per the Internet search, correspond both to the International Committee for the Support of the Final Prophet (ICSFP) and the Office of the Campaign to Defend the Prophet. The query also indicates that **AL-BUTHE** is the President of the ICSFP. [Source: Internet query printout relating to telephone numbers 966-120066331 and 253-981-9150, Exhibit 207]

[redacted]

[46] (U) GX 10B3A, Copy of Ali Al-Timimi Telephone Intercept Linesheet, Exhibit 205. "FNU LNU" refers to First Name Unknown, Last Name Unknown.

[redacted]

(U) CONCLUSION

(U) **AL-BUTHE** should be determined to be subject to Executive Order 13224 for the following reason:

- By serving as a senior AHF official, **AL-BUTHE** has acted for or on behalf of, has assisted in, sponsored, or provided financial, material, or technological support for, or financial or other services to or in support of **Al Qaida** and other SDGTs.

(U) **AHF-OREGON** should be determined to be subject to Executive Order 13224 for the following reasons:

- **AHF-OREGON** has been owned or controlled by, or has acted for or on behalf of **Al-Aqil**.
- **AHF-OREGON** has been owned or controlled by, or has acted for or on behalf of **AL-BUTHE**.
- As a branch of the Saudi charity Al-Haramain Islamic Foundation, **AHF-OREGON** has acted for or on behalf of, or has assisted in, sponsored, or provided financial, material, or technological support for, or financial or other services to or in support of **Al Qaida** and other SDGTs.

[redacted]