UNITED STATES COURT OF APPEALS

FOR THE SECOND CIRCUIT

August Term, 2009

(Submitted: April 29, 2010 Decided: December 20, 2010)

Docket Nos. 09-1375-cr (L), 09-1384-cr (XAP)

UNITED STATES OF AMERICA,

Appellee,

—v.—

HASSAN ABU-JIHAAD, also known as Paul R. Hall,

Defendant-Appellant.[*]

Before:

RAGGI, HALL, and CHIN, *Circuit Judges.*

Appeal from a judgment of conviction entered after a jury trial in the United States District Court for the District of Connecticut (Mark R. Kravitz, *Judge*), at which defendant Hassan Abu-Jihaad was found guilty of communicating national defense information respecting the movements of a United States Navy battlegroup to unauthorized persons in violation of 18 U.S.C. § 793(d). Defendant contends that (1) inculpatory evidence procured

[*] The Clerk of the Court is directed to amend the caption to read as shown above.

pursuant to the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 et seq., should have been suppressed because (a) that statute is unconstitutional and (b) in any event, was not complied with in this case; (2) erroneous evidentiary rulings deprived him of a fair trial; (3) the trial evidence was insufficient to support conviction; and (4) the district court abused its discretion in entering protective orders pursuant to the Classified Information Procedures Act, 18 U.S.C. app. 3, §§ 1-16. We reject these arguments as without merit.

AFFIRMED.

DAN E. LABELLE, Halloran & Sage LLP, Westport, Connecticut, *for Defendant-Appellant*.

WILLIAM J. NARDINI, ALEXIS COLLINS, Assistant United States Attorneys (Stephen Reynolds, Assistant United States Attorney; David Kris, Assistant Attorney General, National Security Division; John De Pue, Senior Litigation Counsel, Counterterrorism Section, U.S. Department of Justice, Washington, D.C., *on the brief*), *on behalf of* Nora R. Dannehy, United States Attorney for the District of Connecticut, New Haven, Connecticut, *for Appellee*.

REENA RAGGI, *Circuit Judge*:

United States citizen Hassan Abu-Jihaad, whose birth name is Paul Raphael Hall, appeals from a judgment of conviction entered in the United States District Court for the District of Connecticut (Mark R. Kravitz, *Judge*) on April 3, 2009, after a jury found him guilty of having communicated national defense information, specifically, the anticipated movements of a United States Navy battlegroup being deployed to the Persian Gulf, to

unauthorized persons in violation of 18 U.S.C. § 793(d). Presently serving a ten-year prison term for that crime, Abu-Jihaad contends that (1) inculpatory evidence obtained pursuant to the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1801 et seq., should have been suppressed because (a) that statute is unconstitutional and (b) in any event, was not complied with in this case; (2) erroneous evidentiary rulings deprived him of a fair trial; (3) the trial evidence was insufficient to support conviction; and (4) the district court abused its discretion in entering protective orders pursuant to the Classified Information Procedures Act ("CIPA"), 18 U.S.C. app. 3, §§ 1-16.

We identify no merit in any of these arguments and, accordingly, we affirm the judgment of conviction.

I. Background

In 1997, defendant Paul Raphael Hall changed his name to "Hassan Abu-Jihaad," the surname of which translates to "Father of Jihad."[1] This curious choice appears not to have raised any concern in the United States Navy when, in January 1998, Abu-Jihaad enlisted.[2]

---

[1] Jihad has been defined as "a religious war of Muslims against unbelievers in Islam, inculcated as a duty by the Koran and traditions." 8 Oxford English Dictionary 238 (2d ed. 1989). Although jihad is also understood to denote "the struggle against one's evil inclinations or efforts toward the moral uplift of society," 7 Encyclopedia of Religion 4917 (Lindsay Jones ed., 2d ed. 2005), it is in the former sense that the concept has been invoked to support terrorist acts against the United States, see, e.g., United States v. Rahman, 189 F.3d 88, 104-09 (2d Cir. 1999) (detailing Sheikh Omar Abdel Rahman's support for "violent jihad" against the United States). In this case, the jury heard testimony that jihad warriors, known as mujahideen, commonly select noms de guerre.

[2] There can be no question that the United States was then aware that it was a target of jihad terrorism, as evidenced by the February 1993 bombing of the World Trade Center

Indeed, over the course of Abu-Jihaad's military service, from 1998-2002, the Navy would clear defendant to receive classified national defense information. The Navy's trust was misplaced. As the jury found, sometime in early 2001, Abu-Jihaad leaked classified information about the movements of Navy ships destined for the Persian Gulf to unauthorized persons supportive of jihad. Because Abu-Jihaad challenges the sufficiency of the evidence supporting the jury verdict, we discuss that evidence in some detail.

A. Discovery of the Classified Information in a London Search

The first link in the chain of circumstantial evidence proving Abu-Jihaad's guilt was discovered in London where, on December 2, 2003, British authorities conducted searches of various locations associated with Babar Ahmad, an information technologist at London's Imperial College with ties to Azzam Publications.

1. Azzam Publications' Support for *Jihad*

London-based Azzam Publications ("Azzam") was an organization that in 2001 maintained a number of websites that glorified martyrdom in the name of jihad and the violent exploits of mujahideen around the world. See United States v. Abu-Jihaad, 600 F. Supp. 2d 362, 366 (D. Conn. 2009) (reviewing trial evidence in denying post-verdict motions

---

in New York City, see United States v. Yousef, 327 F.3d 56, 78-79 (2d Cir. 2003); foiled plots in June 1993 and January 1995 to bomb United States aircraft en route from Asia and New York City bridges, tunnels, and buildings, see id. at 79; United States v. Rahman, 189 F.3d at 109-11, 155; and the June 1996 bombing of the Khobar Towers, a residential complex on a United States military base in Dhahran, Saudi Arabia, see Estate of Heiser v. Islamic Republic of Iran, 659 F. Supp. 2d 20, 22 (D.D.C. 2009).

for judgment of acquittal or new trial).[3] Its name paid tribute to Sheikh Abdullah Azzam, a leader in urging the revival of violent jihad in the twentieth century. In addition to marketing jihadist audio and video recordings on its websites, Azzam offered English translations of books written by Sheikh Azzam. It also provided access to the 1996 fatwa issued by Osama bin Laden, entitled a "Declaration of War Against the Americans Occupying the Land of the Two Holy Places," which charged Muslims to take up arms against the United States to rid the Arabian Peninsula of "infidels." Id. at 367. It solicited assistance for jihadist groups, for example, requesting that readers aid the Taliban "by sending money or gas masks, or traveling to Afghanistan to provide battlefield medical services" in anticipation of an offense by American and Russian forces in retaliation for the October 2000 attack on the U.S.S. Cole. Id. at 366-67.[4] One of Azzam's most popular postings instructed Muslims living in Western countries as to how they, too, could train as mujahideen.

---

[3] This is only one of a number of thoughtful published and unpublished opinions filed by the district court in this case. Others include United States v. Abu-Jihaad, 531 F. Supp. 2d 299 (D. Conn. 2008) (addressing FISA challenge); United States v. Abu-Jihaad, No. 07 Cr. 57, 2008 WL 282368 (D. Conn. Jan. 31, 2008) (ruling on admissibility of recorded statements); United States v. Abu-Jihaad, 553 F. Supp. 2d 121 (D. Conn. 2008) (ruling on admissibility of expert, videotape, and website evidence); United States v. Abu-Jihaad, No. 07 Cr. 57, 2008 WL 346121 (D. Conn. Feb. 4, 2008) (ruling on first CIPA motion); United States v. Abu-Jihaad, No. 07 Cr. 57, 2008 WL 596200 (D. Conn. Feb. 22, 2008) (ruling on second CIPA motion).

[4] On October 12, 2000, Islamic terrorists in a small boat laden with explosives attacked the U.S.S. Cole, a Navy destroyer, off the coast of Yemen, killing seventeen members of the ship's crew. See The Nat'l Comm'n on Terrorist Attacks Upon the U.S., The 9/11 Commission Report 190-91 (2004).

2. The December 2, 2003 Discovery of the Battlegroup Document

In the course of searching Babar Ahmad's bedroom on December 2, British authorities discovered a computer disk containing materials related to Azzam.[5] Of particular significance to this case was a file denominated "letter.doc," which contained a three-page unsigned document describing the anticipated spring 2001 deployment of ten U.S. Navy ships carrying approximately 15,000 sailors and marines from the Pacific coast of the United States to the Persian Gulf ("the Battlegroup Document"). Id. at 367. The significance of the Battlegroup Document is best illustrated by quoting it directly.[6] The first page states as follows:

> In the coming days the United States will be deploying a large naval/marine force to the Middle East.
>
> This will be a two group force: the Battle Group (BG) and the Amphibious Readiness Group (ARG) – these groups will be replacing the already deployed groups in the gulf.
>
> The BG mission is to hold up the sanctions against Iraq, e.g. patrolling the No-Fly Zone, carry out Maritime Interception Operations (MIO) or launch strikes.

---

[5] For example, one of the files on the seized disk, entitled "FOR THE GUY IN CHARGE TO READ (01_08_01).zip," provided passwords for Azzam's various email accounts and instructions for the management of Azzam's video and book inventory. United States v. Abu-Jihaad, 600 F. Supp. 2d at 369 & n.4.

[6] At the beginning of the Battlegroup Document, a statement appears in brackets: "[Necessary changes made in grammar and spelling and for the sake of clarity.]," Gov't Ex. 1, signaling that the document was edited by someone other than the original author. Accordingly, the excerpts reproduced here are verbatim, with no attempt to signal, much less correct, grammar, spelling, or punctuation errors, and with highlighting appearing as in the document.

> There is a possibility that the ships and submarines that are capable will carry out a strike against Afghanistan. Main targets: Usama and the Mujahideen, Taliban, etc.
>
> A two star admiral, COMCRUDESRON 1 (his title), a high ranking officer of the BG said that "there will be certain ships of this BG sitting off the coast of Pakistan with 'launch pads.'"
>
> Most of the ships that are part of the BG will deploy on March 15 2001 leaving their home ports out of California and Washington State. They will meet up with the other ships that are part of the BG which are stationed in Hawaii. Their first port stop is Hawaii on March 20 2001, where some ships will load Tomahawk D missiles. The same missles used on Afganistan and Sudan. It has a warhead and 166 [mm?] fragment bomblets. Then the whole BG will head towards Austrailia. The main ship with high ranking officials will be at Sydney on April 6 2001, other ships – Melbourne, Perth, Bunbary etc. The BG will be going through the straits of Hormuz on the April 29 2001 at night, cutting off certain "infocoms" and "Emcoms" to divert their enemies on how many ships are actually coming through. This will be a night time set-up.

Gov't Ex. 1.

Immediately beneath this text is a diagram showing a two-column formation in which identified ships in the battlegroup, including the aircraft carrier U.S.S. Constellation[7] and the destroyer U.S.S. Benfold – on which Abu-Jihaad served as a signalman – were expected to enter the Strait of Hormuz. Following the diagram are brief descriptions of the capabilities of each ship. For example, with respect to the battlegroup ships, the document states:

> **1. USS Constellation (CV 64) Kitty Hawk Class carrier**
> Personnel: 5,500 to 6,000
> Special team: onboard Explosive Ordnance Disposal team (EOD)
> Mission: No-fly zone, patrol, etc.

[7] Hereafter, we will refer to all ships at issue as "the Constellation battlegroup" or, simply, "the battlegroup."

2. USS Chosin (CG-65) Ticonderoga class
Personnel: 350 to 400
Specialisation: anti-air warfare
Plus carrier escort all these ships

3. Kinkaid (DD965) Sprvance class3
Personnel: 300-350
Specialisation: MIO etc

4. USS Benfold (DDG-65) Arleigh Burke class
Personnel: 300
Multi-capable ship
. . .

7. USS Rainer (AOE-7)
Personnel: 400 to 500
Ammo and fuel replenishing ship for the BG.

Id. With respect to the Amphibious Readiness Group, the document reveals that three ships were expected to deploy "out of homeport San Diego, March 14 2001" with a port visit in South-East Asia, specifically, in Thailand and Singapore, before heading to the Middle East.

Id. Among the ships described is the following:

1. USS BOXER (LHD9) com ship, Wasp class
Personnel: 1,500 sailors, 2,500 marines; high ranging officials abroad; also special forces, Navy Seals and Marines Special Unit

Reconnaissance ships carries lots of helos [helicopters?] all kinds.

Id.

The document concludes by identifying the battlegroup's vulnerabilities, highlighting its operation schedule in the Persian Gulf, and then exhorting the recipient to destroy the communication:

Weakness:

They have nothing to stop a small craft with RPG etc, except their Seals' stinger missiles.

Deploy ops in Gulf 29 April – 04 October.

29th APRIL is more likely the day through the Straits. For the whole of March is tax free – a moral booster. Many sailors do not like the Gulf.

Please destroy message.

Id.

Based on forensic analysis of the totality of evidence obtained in the ensuing investigation, a federal agent testified at trial that the disk containing the Battlegroup Document appeared to have been created by British citizen Syed Talha Ahsan, an Azzam employee who handled product backlog. See United States v. Abu-Jihaad, 600 F. Supp. 2d at 369.[8] Further, although the Battlegroup Document was created on April 2, 2001, the diagram depicting the battlegroup's formation was not embedded in the file until April 12, 2001, the date the document was last saved. See id. at 370. On that date, the author field in the document's properties was changed from "S A Ahsan" to "Jon Greene." Id. Forensic analysis revealed that "wiping" software had been used to remove other material from the disk, but federal authorities were unable to recover that material. Id.

In the course of their larger investigation, authorities would recover no other

[8] In support of this conclusion, the agent testified, inter alia, that the metadata in certain computer files recovered from Ahsan's residence matched the metadata contained in the Battlegroup Document.

electronic data from any source revealing trace information pertaining to transmittal of the Battlegroup Document, research into United States naval forces generally or the Constellation battlegroup in particular, or any evidence relating to "Jon Greene."

B. Abu-Jihaad's Transmittal of the Battlegroup Document

To prove Abu-Jihaad's transmittal of the Battlegroup Document (or the information contained therein) to persons at Azzam, the government relied on evidence showing: (1) defendant's access to the information; (2) his communications with Azzam expressing support for jihad; and (3) his implicit admission in a 2006 recorded statement to having disclosed confidential national security information while in the Navy.

1. Defendant's Access to the Transit Plan

The 2001 deployment of the Constellation battlegroup from San Diego to the Middle East was executed pursuant to a Navy transit plan that went through many drafts beginning on September 29, 2000, and continuing through finalization on February 24, 2001. Each of these iterations highlighted the date April 29, 2001, when, just before midnight, the battlegroup would cross the "change of operation control" ("CHOP") point, i.e., enter into the geographic region controlled by the United States Fifth Fleet. Only the final transit plan referenced a stop in Hawaii by a single vessel, the U.S.S. Benfold, to load ammunition. No version of the transit plan specified the date on which the battlegroup would pass through the Strait of Hormuz.[9]

[9] The Battlegroup Document transmitted to Azzam thus correctly identified April 29, 2001, as an important date in the transit plan, but misascribed it to entry into the Strait of

Each iteration of the transit plan was classified "confidential," which denotes "information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe." Exec. Order No. 12,958, § 1.3(3), 60 Fed. Reg. 19,825 (Apr. 17, 1995); see also United States v. Abu-Jihaad, 600 F. Supp. 2d at 377 (noting Navy's operational instructions stating that "precise current or future operational deployment, locations of surface combatant ships, and planned foreign port calls should be classified as 'confidential' until after deployment or the visit has been approved by the host government" (some internal quotation marks omitted)). Retired Rear Admiral David C. Hart, Jr., who commanded the Constellation battlegroup during the time here at issue, explained that the Navy does not disclose anticipated ports of call because ships are particularly vulnerable in such locations. A similar concern counseled against disclosure of plans for ships to travel through areas where their maneuverability was limited, such as the Strait of Hormuz.[10]

Because of these concerns, even among persons assigned to ships in a battlegroup, only those with a "secret" clearance would be given access to a transit plan. Of 300 sailors on board the U.S.S. Benfold, Abu-Jihaad was one of 40 afforded such access by virtue of

---

Hormuz, rather than crossing the CHOP point. The Constellation battlegroup in fact traveled through the Strait a few days later, on May 2-3, 2001.

[10] Thus, Admiral Hart testified that, despite the Battlegroup Document's inaccuracies, its transmittal raised concerns because of its disclosure of "the time frame at which we would be operating in the Fifth Fleet area of responsibility," and its effort to identify "vulnerabilities." Trial Tr. at 633. He stated that if he had known about the unauthorized transmittal, he would have sought "to change the time and nature of our transit through the strait of Hormuz." Id. at 523.

his status as a signalman who worked alongside quartermasters in the preparation of the ship's navigational charts. He did not, however, have access to the Navy's secure intranet for classified information ("SIPRnet"), which contained information even more sensitive to the national defense than that contained in the transit plan. Significantly, the Battlegroup Document revealed no information for which SIPRnet clearance would have been required, thus limiting the likely source of the information it contained to persons with access only to the transit plan.

2. Abu-Jihaad's Communications with Azzam

Even before United States officials received a copy of the seized Battlegroup Document from their British counterparts, federal agents, acting pursuant to court order, had searched various Azzam-affiliated electronic accounts and discovered therein eleven email exchanges in the time frame of August 21, 2000, to September 3, 2001, between Azzam and a United States sailor serving on the U.S.S. Benfold: the defendant Hassan Abu-Jihaad.[11] Abu-Jihaad used both his personal and military email addresses in these communications. In its review of 23,000 Azzam emails, the government discovered only two correspondents with military email addresses: (1) a Navy Commander who commented angrily on Azzam's support for jihad and (2) Abu-Jihaad. Moreover, Abu-Jihaad's military email address was one of the few addresses saved in an Azzam email account address book. In his early emails with Azzam, Abu-Jihaad discussed purchases of various materials, including the videos Martyrs of Bosnia, Russian Hell 2000, Part I, and Chechnya from the Ashes (which included

[11] It appeared that still more emails between Abu-Jihaad and Azzam had been deleted.

the feature Russian Hell 2000, Part II).[12] In later emails, Abu-Jihaad revealed his identity and status as an active duty member of the Navy and his personal support for jihad, even when directed against the United States.

In a July 2001 email sent from Abu-Jihaad's personal email account to qoqaz@assam.com – the email address to which Azzam's websites directed readers to send their messages of support – defendant praised the "martyrdom operation against the uss cole" and the debilitating effect of that action on the United States ("Cole email"). Trial Tr. at 333-34; Gov't Ex. 19. The text of the Cole email, which was retrieved only because it was embedded in Azzam's reply, states as follows:

> i am a muslim station onboard a u.s. warship currently operating depolyed to the arabian gulf. it shall be noted before usama's latest video was viewed by massive people all over the world. that psychological anxiety had already set in on america's forces everywhere. all this is due to the martyrdom operation against the uss cole. since then every warship station either on the western or eastern shores of america who come to operate in the 5th fleet op area has to be given a force protect brief. well during the brief, i attended there was one thing that stuck out like thorns on a rose bush. i do not know who was the originator of this either top brass or an american poitician. well here is his/her statement: "america has Never faced an enemy with no borders, no government, no diplomats, nor a standing army that pledges allegiance to no

[12] Excerpts from these videos were shown to the jury. From Martyrs of Bosnia, the jury heard Sheikh Abdullah Azzam "criticize[] western Muslims for failing to shed any of their own blood in behalf of the cause" and an instruction from a mujahideen leader in Bosnia for "viewers who wanted to contact the mujahideen to do so through Azzam." United States v. Abu-Jihaad, 600 F. Supp. 2d at 372. The excerpts from Russian Hell 2000, Part I and Russian Hell 2000, Part II, depicted combat scenes, including an execution and a suicide truck bombing.

> state." Allahu Akbar! Allahu Akbar![13] i give takbirs [praise to Allah] because i know deep down in my heart that the american enemies that this person has discribe is the Mujahideen Feesabilillah [holy warriors fighting in the cause of Allah]. these brave men are the true champions and soldiers of Allah in this dunya [world]. i understand fully that they are the men who have brong honor to this weak ummah [Islamic community] in the lands of jihad afghanistan, bosnia, chechnya, etc. Alhamdulillah! [Praise to Allah!] With their only mission in life to make Allah's name and laws supreme all over this world. i want to let it be known that i have been in the middle east for almost a total of 3 months. for these 3 months you can truly see the effects of this psychological warfare taking a toll on junior and high ranking officers. but after the latest video supporting palestine. the top brass and american officials were running around like headless chickens very afraid, wondering if there is a possible threat. but this time the american population got wind of this and they came to know just how afraid the u.s. government is. thomas l. friedman wrote an article in the new york times called: "what it takes to make the americans to turn tail, run." this article was distributed on my ship and most of the sailors said it was so true about the american government, and they feel like they are working for a bunch of scary pussies.....a Brother serving a Kuffar [infidel] nation. Astaghfir'Allah [Forgiveness from Allah].... Hassan

Id. at 372-73 (emphasis and bracketed material added by district court). Abu-Jihaad's Azzam correspondent replied in relevant part:

---

[13] The Arabic phrase "Allahu akbar," known as the "takbir" in Arabic, is usually translated as "God is Great." See, e.g., 12 Encyclopedia of Religion, supra, at 8057. Used in Islamic prayer and incorporated into the flags of countries such as Iran and Iraq, the phrase has been appropriated by some jihad terrorists. See, e.g., Notes Found After the Hijackings, N.Y. Times, Sept. 29, 2001, at B3 (reporting that document used by September 11, 2001 hijackers instructed, inter alia, "[w]hen the confrontation begins, . . . [s]hout, 'Allahu Akbar,' because this strikes fear in the hearts of the nonbelievers"); Michael Wilson, Judgment Day in Two High-Profile Cases: Times Square's Would-Be Bomber Is Defiant as He Gets a Life Term, N.Y. Times, Oct. 6, 2010, at A25 (reporting that defendant responded to pronouncement of life sentence with phrase "Allahu akbar"); Benjamin Weiser, In Terrorism Case, a Plea Bargain Secretly in the Making for 2 Years, N.Y. Times, Oct. 24, 2000, at B1, B3 (reporting with respect to prosecution for the 1998 bombings of the United States embassies in Kenya and Tanzania that, "[i]n June 1999, one defendant leapt out of his chair in the courtroom and charged toward Judge Sand, while another defendant screamed 'Allahu akbar,' Arabic for "God is great").

> You said it all, and all I can add is that the Kufar know that they cannot defeat the Mujahideen (the warriors of Allah). I trust that you are doing your best to make sure that the other brothers & sisters in uniform are reminded that their sole purpose of existence in this duniya [world] is purely to worship our Lord and Master, Allah (SWT) [praise being given to Allah].
>
> May Allah be with you & your brothers and sisters and keep you from all harm.
>
> Keep up with the Dawah [preaching Islam] and the psychlogical warefare.

Id. at 373 (bracketed material added by district court).

In the last of the eleven emails recovered by the government, Abu-Jihaad praised Azzam's coverage of the Taliban in Afghanistan, but opined that the Taliban were too lenient in failing to execute foreign aid workers who converted Muslims to other faiths.

None of Abu-Jihaad's recovered emails referenced the Battlegroup Document or the information contained therein.

3. Abu-Jihaad's 2006 Recorded Statements

In 2006, by which time Abu-Jihaad had been out of the Navy for four years and was living in Phoenix, Arizona, Abu-Jihaad's telephone conversations with his friend Derrick Shareef and a confidential informant were intercepted by a court-authorized wiretap. In excerpts of four calls from late 2006 that were played for the jury, Abu-Jihaad revealed his familiarity with Azzam's websites, see Gov't Ex. 141c, and his high degree of concern with "tapped" telephones, Gov't Ex. 141e. Abu-Jihaad stated an intent to "secur[e] myself" to avoid "hand[ing] myself to a Kafir [infidel]." Gov't Ex. 141f. He cautioned those with whom he spoke not to refer to associates by their real names, see Gov't Ex. 141g, and he

frequently employed code, referring to jihad as "J" or "7,"[14] e.g., Gov't Ex. 141c, logistics as "L," e.g., Gov't Ex. 141g, martyrdom operations as "M.O.," e.g., Gov't Ex. 141f, and military intelligence as "meals," e.g., Gov't Ex. 141k.[15] Thus, Abu-Jihaad's references to a "cold meal" meant outdated intelligence, whereas a "fresh meal" or "hot meal" referred to current intelligence. Trial Tr. at 975-76.

In a November 11, 2006 conversation, Abu-Jihaad stated that he no longer had current logistics information: "Now 'L' for me is like a cold meal. 'Cuz it ain't fresh. . . . If it ain't fresh, it's un-fresh and it, it's un-beneficial to you – just put it that way." Gov't Ex. 141g. He repeated this point in a subsequent conversation with Shareef and the confidential informant the same day:

ABU-JIHAAD:	And I said, and I'll say it again, with whatever I can give you, that's beneficial, I'll give it to you. But whatever's cold turkey, if it's cold turkey, I can't give it to you.
CW[16]:	Ak . . .
ABU-JIHAAD:	'Cuz that means that, if it's cold turkey – I'm talking about "L" you figure it out – 'cuz then that means that, that's just saying that, I haven't been on that job, so I don't – you know what I'm saying, I haven't been there . . . to see . . . what the fresh meal is.

[14] It was suggested at trial that the number "7" referred to "seventh heaven," the resting place of Islamic martyrs according to advocates of jihad. Trial Tr. at 962.

[15] The confidential informant testified that, in the recorded conversations, "meals" meant military intelligence, which Shareef and the informant were soliciting from Abu-Jihaad.

[16] "CW" refers to the confidential informant.

SHAREEF: Okay.

ABU-JIHAAD: You understand that?

SHAREEF: Yeah.

CW: Tell him, man I already got brothers . . .

ABU-JIHAAD: If I can't, if I can't give you the fresh meal – I ain't been there in "X" amount of years.

SHAREEF: Yeah, I – I understand what you're saying.

ABU-JIHAAD: See what I'm saying? Now if . . . the Hispanic, if the Mexican, he just, was there a minute ago – he can give you a fresh meal.

SHAREEF: Okay.

ABU-JIHAAD: So you put that together.

. . .

ABU-JIHAAD: If it's – if it's . . . in those terms, he can give you a fresh meal 'cuz, you know what I'm saying, he just finished his job, there, less than a month ago, or . . .

SHAREEF: Okay.

ABU-JIHAAD: . . . two. (LAUGHS). But I, I mean – in those terms and "L's," – I would be giving you a cold meal.

CW: I understand.

SHAREEF: All righty.

ABU-JIHAAD: You got me?

SHAREEF: Yeah, I got you.

ABU-JIHAAD: Because, um – and then I can elaborate on that more if you want me to . . .

CW: No, no . . .

ABU-JIHAAD: . . . to your face – not on the phone. I'm just saying . . . if we . . . you got me?

SHAREEF: Yeah, man . . we good, we good.

ABU-JIHAAD: A fresh meal and a cold meal.

Gov't Ex. 141h at 1-2. The informant testified that when Abu-Jihaad said he had not "been on that job," the informant understood Abu-Jihaad to mean he was no longer in the Navy. By contrast, the informant understood the "Mexican" to be a reference to Miguel Colon, a man who had left the Marine Corps only recently in September 2006.

Still later on November 11, 2006, Abu-Jihaad spoke with Colon about Shareef's wish to procure military intelligence:

ABU-JIHAAD: [H]e wants a hot meal. You know what I'm saying?

COLON: Yeah.

ABU-JIHAAD: I don't know how to get him no hot meal. I told him I, I ain't been working uh, in, in, in the field of making meals and or, you know . . .

COLON: Yeah.

ABU-JIHAAD: . . . in a, in a long time. I've been out of that for, uh, over uh, quatro years you know.

Gov't Ex. 141k at 7. At trial, the government argued that, by explaining his present inability to provide military intelligence by reference to the fact that he had not been "working . . . in

the field of making meals" for four years, Abu-Jihaad was effectively admitting that he had leaked military intelligence while in the Navy.

C. Conviction and Sentencing

Based on the evidence summarized, on March 5, 2008, the jury found Abu-Jihaad guilty of both providing material support to terrorists in violation of 18 U.S.C. § 2339A and communicating national defense information to unauthorized persons in violation of 18 U.S.C. § 793(d). On March 4, 2009, the district court granted Abu-Jihaad's motion for a judgment of acquittal as to the first count and denied the motion as to the second count. See United States v. Abu-Jihaad, 600 F. Supp. 2d at 394, 402.[17] The following month, on April 3, 2009, the district court sentenced Abu-Jihaad on the single count of conviction to the statutory maximum term of ten years' imprisonment, to be followed by three years' supervised release.

This appeal followed.

II. Discussion

A. The FISA Challenge

In securing Abu-Jihaad's conviction, the prosecution relied on certain recorded evidence intercepted pursuant to court orders issued under the Foreign Intelligence

[17] The district court concluded that Abu-Jihaad's provision of information about the Constellation battlegroup could not, as a matter of law, support a conviction for providing material support to terrorism in either of the forms – physical assets or personnel – urged by the government. See United States v. Abu-Jihaad, 600 F. Supp. 2d at 394-402. As the government has not appealed this ruling, we have no reason to consider it in this opinion.

Surveillance Act ("FISA"), 50 U.S.C. § 1801 et seq. Abu-Jihaad submits that the district court erred in refusing to suppress this evidence because (1) on its face, FISA violates the Fourth Amendment; and (2) in any event, the statute's requirements were not satisfied in this case. We identify no merit in either argument.

1. FISA Is Constitutional on Its Face

a. FISA's General Operation

Enacted in 1978, FISA permits the Chief Justice of the United States to designate eleven federal judges as the Foreign Intelligence Surveillance Court ("FISA Court"), see id. § 1803(a)(1), with jurisdiction to entertain ex parte executive applications for electronic surveillance[18] "for the purpose of obtaining foreign intelligence information," id. § 1802(b).[19]

---

[18] Although FISA originally applied only to electronic surveillance, the law was amended in 1994 to extend to physical searches for foreign intelligence information. See Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, 108 Stat. 3444 (1994); see also 50 U.S.C. §§ 1821-29.

[19] FISA defines "foreign intelligence information" as:

> (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against –
>
> > (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
> > (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
> > (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to –

To issue a FISA warrant, a judge must find, inter alia, that there is probable cause to believe that the target of the surveillance is a "foreign power or an agent of a foreign power" and that the place or facilities to be surveilled are "being used, or . . . about to be used, by a foreign power or an agent of a foreign power." Id. § 1805(a)(2).[20]

(A) the national defense or the security of the United States; or
(B) the conduct of the foreign affairs of the United States.

50 U.S.C. § 1801(e).

As amended in 2001, FISA requires an application for a surveillance warrant to include, inter alia, a certification from a high-ranking executive official:

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

Id. § 1804(a)(6). As discussed infra, subsection (B) – the "significant purpose" clause – is at the core of Abu-Jihaad's constitutional challenge to FISA.

[20] FISA defines "foreign power" to mean

> (1) a foreign government or any component thereof, whether or not recognized by the United States;
> (2) a faction of a foreign nation or nations, not substantially composed of United States persons;
> (3) an entity that is openly acknowledged by a foreign government or

governments to be directed and controlled by such foreign government or governments;
(4) a group engaged in international terrorism or activities in preparation therefor;
(5) a foreign-based political organization, not substantially composed of United States persons;
(6) an entity that is directed and controlled by a foreign government or governments; or
(7) an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction.

50 U.S.C. § 1801(a).

FISA defines "agent of a foreign power" to mean

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

(A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section;
(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities;
(C) engages in international terrorism or activities in preparation therefore;
(D) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor; or
(E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor for or on behalf of a foreign power; or

(2) any person who–

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a

Rulings by the FISA Court are subject to review by the Foreign Intelligence Surveillance Court of Review ("FISA Review Court"), comprised of three judges also designated by the Chief Justice. See id. § 1803(b). The FISA Review Court has convened only twice since the statute's enactment: (1) when it heard and rejected a constitutional challenge to FISA not dissimilar to that pursued by Abu-Jihaad in this case, see In re Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002); and (2) when it heard and rejected an as-applied constitutional challenge to certain provisions of the Protect America Act of 2007 ("PAA"), Pub. L. No. 110-55, 121 Stat. 552, that permitted the executive to conduct warrantless foreign intelligence surveillance on targets reasonably believed to be located outside the United States, see In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act (In re FISA Section 105B Directives), 551 F.3d 1004 (FISA Ct. Rev.

> violation of the criminal statutes of the United States;
> (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
> (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;
> (D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or
> (E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

Id. § 1801(b).

2008).[21]

b. The PATRIOT Act's Amendment of FISA's Purpose Certification Requirement

As originally enacted, FISA required a high-ranking member of the executive branch to certify that "the purpose" for which a warrant was being sought was to obtain "foreign intelligence information." 50 U.S.C. § 1804(a)(7)(B) (Supp. V 1981).[22] Referencing this language in United States v. Duggan, 743 F.2d 59 (2d Cir. 1984), we observed that "the requirement that foreign intelligence information be the primary objective of the surveillance is plain not only from the language of § 1802(b) but also from the requirements in § 1804 as to what the application must contain." Id. at 77 (emphasis added). Duggan rejected a Fourth Amendment challenge to the procedures established by FISA for issuance of foreign intelligence surveillance warrants, see id. at 72-74, a decision we recently had occasion to reaffirm in United States v. Stewart, 590 F.3d 93 (2d Cir. 2009).

In 2001, Congress amended FISA as part of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("PATRIOT Act"), Pub. L. No. 107-56, 115 Stat. 271 (2001). Among other things, Congress

---

[21] The PAA provisions at issue in In re FISA Section 105B Directives, which were codified at 50 U.S.C. §§ 1805a-1805c, were subject to a February 16, 2008 sunset and were repealed on July 10, 2008, as part of the FISA Amendments Act of 2008, Pub. L. No. 110-261, § 403, 122 Stat. 2436, 2473-74.

[22] A 2008 amendment to FISA renumbered certain FISA provisions. Among other changes, it redesignated former subsection (a)(7) as subsection (a)(6). See Pub. L. No. 110-261, § 104(1)(B), 122 Stat. at 2461. Unless otherwise noted, references herein conform to the present statutory numbering.

indicated that it did not, in fact, require foreign intelligence gathering to be the primary purpose of the requested surveillance to obtain a FISA warrant. Rather, upon satisfaction of all other FISA requirements, Congress authorized FISA Court judges to issue warrants upon executive certification that acquisition of foreign intelligence information is "a significant purpose" of the requested surveillance. See id. § 218, 115 Stat. at 291 (codified as amended at 50 U.S.C. § 1804(a)(6)(B)) (emphasis added).

Because neither Duggan nor Stewart considered FISA's constitutionality in light of the statute's amendment by the PATRIOT Act, Abu-Jihaad submits that we must address the question of constitutionality yet again. Specifically, Abu-Jihaad submits that the primary purpose requirement is, in fact, essential to the constitutionality of FISA, lest the government misuse the statute to procure warrants for criminal investigations without demonstrating the probable cause essential to that latter purpose, i.e., probable cause to believe "that an individual is committing, has committed, or is about to commit a particular offense" and that "particular communications concerning that offense will be obtained through" the surveillance. See 18 U.S.C. § 2518(3)(a)-(b) (stating probable cause required by Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, 82 Stat. 197 (codified as amended at 18 U.S.C. §§ 2510-2522)).

In support of his challenge, Abu-Jihaad cites Mayfield v. United States, 504 F. Supp. 2d 1023 (D. Or. 2007) (holding FISA in violation of Fourth Amendment). That district court decision, however, has now been vacated by the Ninth Circuit on standing grounds. See

Mayfield v. United States, 599 F.3d 964, 973 (9th Cir. 2010). Meanwhile, all other courts that have considered the issue, both before and after enactment of the PATRIOT Act, have rejected constitutional challenges to FISA. See United States v. Ning Wen, 477 F.3d 896, 898 (7th Cir. 2007); United States v. Damrah, 412 F.3d 618, 625 (6th Cir. 2005); In re Sealed Case, 310 F.3d at 742-46; United States v. Johnson, 952 F.2d 565, 573 (1st Cir. 1991); United States v. Pelton, 835 F.2d 1067, 1075 (4th Cir. 1987); United States v. Cavanagh, 807 F.2d 787, 790-92 (9th Cir. 1987); United States v. Kashmiri, No. 09 Cr. 830-4, 2010 WL 4705159, at *3-5 (N.D. Ill. Nov. 10, 2010); United States v. Warsame, 547 F. Supp. 2d 982, 993 (D. Minn. 2008); United States v. Mubayyid, 521 F. Supp. 2d 125, 135-41 (D. Mass. 2007); United States v. Holy Land Found. for Relief & Dev., No. 04 Cr. 240, 2007 WL 2011319, at *5-6 (N.D. Tex. July 11, 2007); United States v. Jayyousi, No. 04 Cr. 60001, 2007 WL 851278, at *1 (S.D. Fla. Mar. 15, 2007); United States v. Benkahla, 437 F. Supp. 2d 541, 554 (E.D. Va. 2006); United States v. Marzook, 435 F. Supp. 2d 778, 786 (N.D. Ill. 2006); United States v. Nicholson, 955 F. Supp. 588, 590-91 (E.D. Va. 1997); In re Kevork, 634 F. Supp. 1002, 1014 (C.D. Cal. 1985); United States v. Falvey, 540 F. Supp. 1306, 1312 (E.D.N.Y. 1982). We do the same here.

As we discuss more fully in this opinion, the Fourth Amendment warrant requirement demands a showing of probable cause reasonable to the purpose being pursued. Thus, identification of purpose is necessary to assess the reasonableness of the probable cause standards at issue. Where multiple purposes are significant to an investigation, however, the

Fourth Amendment does not require the government to identify a primary purpose or limit its ability to secure a warrant to satisfaction of the standards for that purpose. Rather, the government may secure a warrant under the probable cause standards applicable to any purpose that it pursues in good faith.[23] Thus, we identify no constitutional defects in FISA's certification requirement of "a significant" rather than a primary "purpose . . . to obtain foreign intelligence information." 50 U.S.C. § 1804(a)(6)(B).

c. The "Primary Purpose" Requirement's Origins as a Limit on the Executive's Claimed Inherent Authority to Conduct *Warrantless* Surveillance for Foreign Intelligence Information

To explain the basis for our decision, we begin by noting that the "primary purpose" requirement urged by Abu-Jihaad was originally formulated to address a constitutional concern not present in this case: the scope of presidential authority to conduct warrantless foreign intelligence surveillance. In United States v. United States District Court (Keith), 407 U.S. 297 (1972), the Supreme Court rejected a claim of inherent executive authority to conduct warrantless domestic security surveillance, while specifically not deciding the scope of executive authority to conduct surveillance "with respect to activities of foreign powers or their agents," id. at 321-22 (emphasis added). The Fourth Circuit addressed that question in United States v. Truong Dinh Hung, 629 F.2d 908 (4th Cir. 1980), a case involving

[23] We need not here decide how the purpose for which a warrant is sought might inform the duty to minimize the interception of material not relevant to that purpose. The FISA record in this case, which both the district court and this court have carefully reviewed, raises no minimization concerns.

warrantless foreign intelligence surveillance conducted before enactment of FISA, and resolved it favorably to the executive: "the Executive Branch need not always obtain a warrant for foreign intelligence surveillance," id. at 913. At the same time, however, the court ruled that the executive's power to act without a warrant was cabined by the Article II authority over foreign affairs from which it derived. Thus, Truong held that warrantless foreign intelligence surveillance was constitutionally authorized only with respect to "a foreign power, its agent or collaborators" and when "conducted 'primarily' for foreign intelligence reasons." Id. at 915. Some twenty-eight years later, however, the FISA Review Court declined to impose a comparable primary purpose requirement on the warrantless surveillance provisions of the PAA, applicable to foreign powers or agents of foreign powers reasonably believed to be located outside the United States. See In re FISA Section 105B Directives, 551 F.3d at 1010-12 (holding that "more appropriate consideration" is whether "programmatic purpose of the surveillances . . . involves some legitimate objective beyond ordinary crime control").

We have no occasion here to consider these warrantless surveillance decisions. We note simply that there is an important distinction between warrantless surveillances premised exclusively on executive authority, and surveillances pursuant to warrants issued by courts in compliance with standards enacted by Congress. The former require identification of an exception to the Fourth Amendment's warrant requirement. See United States v. Duggan, 743 F.2d at 72 (collecting cases recognizing such exception); see also In re FISA Section

105B Directives, 551 F.3d at 1011-12. By contrast, the latter implement that requirement. Whatever purpose limits might be placed on the president's authority to conduct warrantless surveillance to ensure that the exception does not extend beyond the constitutional ground for its recognition, it does not follow that the Fourth Amendment demands the same limitation when, as under FISA, the powers of all three branches of government – in short, the whole of federal authority – are invoked in determining when warrants may reasonably be sought and issued for the purpose of obtaining foreign intelligence information. Cf. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 635-37 (1952) (Jackson, J., concurring).

d. The Fourth Amendment's Warrant Requirement Is Flexible.

As this court has recognized, the Constitution's warrant requirement is "flexible," so that "different standards may be compatible with the Fourth Amendment in light of the different purposes and practical considerations" at issue. United States v. Duggan, 743 F.2d at 72. Thus, when a warrant is sought for the purpose of investigating "ordinary crime," the Fourth Amendment requires a showing of probable cause to believe that the target of the warrant "is committing, has committed, or is about to commit a particular offense," and that "particular communications concerning that offense will be obtained through" the surveillance. 18 U.S.C. § 2518(3)(a)-(b); see Dalia v. United States, 441 U.S. 238, 255 (1979). But when the government pursues a different purpose, such as obtaining security intelligence, "[d]ifferent standards" of probable cause reasonable to that purpose may

support issuance of a warrant. See Keith, 407 U.S. at 322-23.

The considerations that the Supreme Court identified in Keith as distinguishing domestic security surveillance from the surveillance of "ordinary crime" and, therefore, as supporting different warrant standards, pertain equally to foreign intelligence surveillance:

> The gathering of security intelligence is often long range and involves the interrelation of various sources and types of information. The exact targets of such surveillance may be more difficult to identify than in surveillance operations against many types of crime specified in Title III. Often, too, the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency. Thus, the focus of domestic surveillance may be less precise than that directed against more conventional types of crime.

Id. at 322. Also noteworthy is Keith's recognition of Congress's particular competence to weigh these considerations and to establish reasonable warrant requirements for security surveillance, as distinct from those already prescribed for specified crimes in Title III. See id. at 322-23.

The benchmark for judicial review of the constitutionality of warrant requirements established by Congress is reasonableness: "Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens." Id. at 322-23. Consistent with this pronouncement, the Court in Keith observed that Congress might well judge that the application and affidavit showing probable cause for security surveillance "need not follow the exact requirements of [18 U.S.C.] § 2518 but should allege other

circumstances more appropriate to domestic security cases; that the request for prior court authorization could, in sensitive cases, be made to any member of a specially designated court . . .; and that the time and reporting requirements need not be so strict as those in § 2518." Id. at 323.

This discussion in Keith informed our decision in United States v. Duggan, 743 F.2d at 72-74, upholding the warrant standards established by Congress in FISA for court-ordered surveillance to obtain foreign intelligence information. The PATRIOT Act did not modify the standards FISA applies to warrant applications for the purpose of obtaining foreign intelligence. Rather, it modified the degree to which foreign intelligence gathering must be the purpose of the surveillance. Thus, we need not here reconsider Duggan's holding as to the reasonableness of FISA's warrant standards for the purpose of obtaining foreign intelligence information.[24] We need consider only whether any constitutional concerns are

[24] To the extent Abu-Jihaad asserts that Duggan did not explicitly address the reasonableness of FISA's notice and duration requirements, we here clarify that these standards raise no Fourth Amendment concerns. As the FISA Review Court observed, Congress determined that "'[t]he need to preserve secrecy for sensitive counterintelligence sources and methods justifies elimination of the notice requirement'" in FISA. In re Sealed Case, 310 F.3d at 741 (quoting S. Rep. No. 95-701, at 12 (1978)). The reasonableness of the concern is obvious. See United States v. Belfield, 692 F.2d 141, 144 n.8 (D.C. Cir. 1982) (recognizing that "notice that the surveillance has been conducted, even years after the event, may destroy a valuable intelligence advantage"). Further, the same reasons that informed our rejection of a challenge to ex parte, in camera review of questioned evidence in In re Terrorist Bombings of U.S. Embassies in East Africa, – specifically, "the imperatives of national security and the capacity of in camera procedures to adequately safeguard . . . Fourth Amendment rights," 552 F.3d 157, 166 (2d Cir. 2008) (internal quotation marks and brackets omitted) – support a conclusion that FISA's limited notice requirement does not render the statute's warrant standards unconstitutional.

raised by Congress's decision to allow FISA warrant standards to apply upon the executive's certification that a "significant" rather than a "primary" purpose of the surveillance is to obtain foreign intelligence information.

e. A "Significant" Rather than "Primary" Purpose to Obtain Foreign Intelligence Information Does Not Render FISA's Warrant Standards Unreasonable

(1) *Duggan* Recognized "Primary" Purpose as a Matter of Statutory Construction not Constitutional Mandate

In concluding that the "significant purpose" certification requirement does not raise constitutional concerns, we note that when, in Duggan, we construed FISA's original reference to electronic surveillance for "the purpose" of obtaining foreign intelligence information," as a "requirement that foreign intelligence information be the primary objective

---

Similarly, the fact that FISA authorizes surveillance for a longer period than Title III, compare 50 U.S.C. § 1805(d)(1) (authorizing surveillance of U.S. person for up to 90 days) with 18 U.S.C. § 2518(5) (authorizing surveillance for up to 30 days), is not unreasonable in light of "the nature of national security surveillance, which is 'often long range and involves the interrelation of various sources and types of information,'" In re Sealed Case, 310 F.3d at 740 (quoting Keith, 407 U.S. at 322). Berger v. New York, 388 U.S. 41 (1967), relied on by Abu-Jihaad, is not to the contrary. In invalidating New York's wiretap statute on Fourth Amendment grounds, Berger cast doubt, inter alia, on the law's 60-day duration provision. See id. at 59. Although "Title III was enacted, in large part, to meet the restrictions imposed on electronic surveillance practices and procedures by Berger," United States v. Figueroa, 757 F.2d 466, 471 (2d Cir. 1985), Berger's focus was on the proper bounds of surveillance in an ordinary criminal case. As the Supreme Court subsequently recognized in Keith, to address national security concerns, Congress could constitutionally enact surveillance legislation in which "the time and reporting requirements" might "not be so strict" as those in Title III. See 407 U.S. at 323. Thus, we conclude that Congress's decision to permit FISA surveillance of a U.S. person to be authorized for up to 90 days is reasonable in light of the purpose being pursued.

of [any court-ordered] surveillance," id. at 77 (emphasis added), we were identifying Congress's intent in enacting FISA, not a constitutional mandate, see generally W.R. Grace & Co.-Conn. v. Zotos Int'l, Inc., 559 F.3d 85, 88 (2d Cir. 2009) (recognizing obligation "to look to the plain language of the statute to effectuate the intent of Congress"). This is evident from the fact that we articulated this construction in the context of determining whether the surveillance at issue in Duggan was conducted in accordance with FISA's terms, not in the context of our earlier, and separate, determination of FISA's constitutionality. See United States v. Duggan, 743 F.2d at 71-74. In short, nothing in Duggan erected a constitutional bar to Congress reconsidering and reframing the purpose requirement of FISA as long as it maintained warrant standards that in their totality were "reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens." Keith, 407 U.S. at 323.[25]

(2) Considerations Prompting Congress's Adoption of the "Significant" Purpose Amendment

In considering Congress's decision to allow FISA standards to be triggered by a

[25] Insofar as a footnote in United States v. Truong Dinh Hung, 629 F.2d at 914 n.4, could be read to conclude that the dual requirements it established for warrantless foreign intelligence surveillance – a foreign power target and a "primarily" foreign intelligence purpose, see id. at 915 – would also be required for court-ordered surveillance, the conclusion appears to be dictum and, in any event, is not binding on this court. Further, the conclusion was expressed before concerns arose that satisfaction of the "primary purpose" requirement effectively precluded the coordination of intelligence and law enforcement efforts in ensuring national security. We discuss these concerns further in the next section of this opinion.

showing of a "significant" rather than "primary" purpose of obtaining foreign intelligence information, we may properly consider the "practical considerations" informing that choice. See Keith, 407 U.S. at 322 (observing that different standards may be compatible with the Fourth Amendment in light of the "different policy and practical considerations" at issue); see also United States v. Duggan, 743 F.2d at 72. The relevant background is discussed in detail in In re Sealed Case, 310 F.3d at 722-29. We summarize it here only as necessary to highlight two considerations that emerged from years of Justice Department experience trying to satisfy the "primary purpose" requirement and that informed Congress's amendment of FISA's purpose certification provision: (1) if intelligence and law enforcement officials coordinate efforts in pursuing national security inquiries, it can be difficult, if not impossible, to identify whether their "primary" purpose is to obtain foreign intelligence information or evidence of a crime; and (2) the segregation of intelligence and law enforcement officials to ensure the executive's ability to certify a "primary" foreign-intelligence-gathering purpose can compromise national security.

FISA's original purpose certification requirement was not uniformly construed by the courts. Although we thought it clear that the statute's original reference to "the purpose" to obtain foreign intelligence information referenced the primary purpose, United States v. Duggan, 743 F.2d at 77, the First Circuit construed the requirement in the negative, holding that "the investigation of criminal activity cannot be the primary purpose" of a surveillance order under FISA, United States v. Johnson, 952 F.2d at 572. Meanwhile, the Ninth Circuit

hesitated to define FISA's purpose requirement "to draw too fine a distinction between criminal and intelligence investigations," noting that "'[i]nternational terrorism,' by definition, requires the investigation of activities that constitute crimes." United States v. Sarkissian, 841 F.2d 959, 965 (9th Cir. 1988). The FISA Review Court echoed this concern in In re Sealed Case, questioning the soundness of any purpose certification standard that assumed "that the government seeks foreign intelligence information (counterintelligence) for its own sake – to expand its pool of knowledge." 310 F.3d at 727. It concluded that "FISA as passed by Congress in 1978 clearly did not preclude or limit the government's use or proposed use of foreign intelligence information, which included evidence of certain kinds of criminal activity, in a criminal prosecution." Id.

In United States v. Duggan, we had "emphasize[d]" this same point, even though we construed "the purpose" requirement of FISA to mean "primary purpose":

> [O]therwise valid FISA surveillance is not tainted simply because the government can anticipate that the fruits of such surveillance may later be used, as allowed by § 1806(b), as evidence in a criminal trial. Congress recognized that in many cases the concerns of the government with respect to foreign intelligence will overlap those with respect to law enforcement.

743 F.2d at 78. We concluded that where information sought through FISA surveillance "involved international terrorism[,] . . . the fact that domestic law enforcement concerns may also have been implicated did not eliminate the government's ability to obtain a valid FISA order." Id.

In the years after our decision in Duggan, this important point became muddled, if not

lost. In 1995, the Justice Department not only committed itself to satisfying the primary purpose test but, "[a]pparently to avoid running afoul" of that test, it adopted procedures limiting contacts between intelligence and law enforcement officials. See In re Sealed Case, 310 F.3d at 727-28 (noting that procedures "eventually came to be narrowly interpreted within the Department of Justice" so as to erect a "wall" to "prevent the FBI intelligence officials from communicating with the Criminal Division regarding ongoing [intelligence] investigations"); see also The Nat'l Comm'n on Terrorist Attacks Upon the U.S., The 9/11 Commission Report 78-80 (2004) (discussing constraints imposed by "primary purpose" requirement on sharing of intelligence information between prosecutors and intelligence agents). Moreover, as the FISA Court became aware of these Justice Department procedures for segregating intelligence and criminal investigative officials, it "adopted elements of them" into certain of its orders. In re Sealed Case, 310 F.3d at 728.[26] The net result was to shift "the focus" of FISA surveillance applications from the "purpose of the surveillance" to "the nature of the underlying investigation." Id.

As the FISA Review Court observed, these practices imposed a cost on national security. See id. at 744 & n.29 (citing congressional hearings indicating that practices implemented to segregate intelligence from law enforcement officials to avoid running afoul

[26] For example, the order vacated by the FISA Review Court in In re Sealed Case prohibited law enforcement officials, inter alia, from making any recommendations to intelligence officials respecting "the initiation, operation, continuation, or expansion of FISA searches or surveillances." See 310 F.3d at 720 n.3.

of primary purpose test "may well have contributed, whether correctly understood or not, to the FBI missing opportunities to anticipate the September 11, 2001 attacks"). In the aftermath of September 11, 2001, the executive asked Congress to substitute "a purpose" for "the purpose" requirement of FISA so as to allow it to dismantle the wall between intelligence and law enforcement personnel erected to ensure that the primary purpose of any FISA surveillance or search was to obtain foreign intelligence information and not evidence of crime. Id. at 732.

Congress did not accept the executive's proposed language, but it did agree that certification of a primary purpose to obtain foreign intelligence information should not be required to secure a FISA warrant. Although no committee reports accompanied the PATRIOT Act, Senator Feinstein, one of the act's strong supporters, provided a cogent floor statement as to the reasons for recasting FISA's purpose certification requirement:

> Under current law, authorities can proceed with surveillance under FISA only if the primary purpose of the investigation is to collect foreign intelligence.
>
> But in today's world things are not so simple. In many cases, surveillance will have two key goals – the gathering of foreign intelligence, and the gathering of evidence for a criminal prosecution. Determining which purpose is the "primary" purpose of the investigation can be difficult, and will only become more so as we coordinate our intelligence and law enforcement efforts in the war against terror.
>
> Rather than forcing law enforcement to decide which purpose is primary – law enforcement or foreign intelligence gathering, this bill strikes a new balance. It will now require that a "significant" purpose of the investigation must be foreign intelligence gathering to proceed with surveillance under FISA.
>
> The effect of this provision will be to make it easier for law enforcement to

> obtain a FISA search or surveillance warrant for those cases where the subject of the surveillance is both a potential source of valuable intelligence and the potential target of a criminal investigation. Many of the individuals involved in supporting the September 11 attacks may well fall into both of these categories.

147 Cong. Rec. S10591 (Oct 11, 2001) (quoted in In re Sealed Case, 310 F.3d at 732-33).

To address these practical considerations – i.e., the difficulty in identifying the primary purpose when surveillance is pursued jointly by intelligence and law enforcement officials, and the importance of such joint efforts to protect national security – Congress in the PATRIOT Act amended FISA to provide that, upon satisfaction of all other statutory requirements, FISA warrants could be issued on certification "that a significant purpose of the surveillance is to obtain foreign intelligence information." See Pub. L. No. 107-56, § 218, 115 Stat. at 291 (codified as amended at 50 U.S.C. § 1804(a)(6)(B)). In a separate amendment, Congress expressly authorized federal officers conducting surveillance with the aim of obtaining foreign intelligence information to coordinate their activities with law enforcement officers. See Pub. L. No. 107-56, § 504, 115 Stat. at 364 (codified as amended at 50 U.S.C. § 1806(k)(1)) ("Federal officers who conduct electronic surveillance to acquire foreign intelligence information under this title may consult with Federal law enforcement officers or law enforcement personnel of a State or political subdivision of a State . . . to coordinate efforts to investigate or protect against [, inter alia, actual or potential attack by a foreign power or agent of a foreign power, sabotage, international terrorism, or other clandestine intelligence activities by a foreign power or agent of a foreign power]."). In so

doing, Congress made clear that such coordination would preclude neither a finding that FISA's "significant purpose" certification requirement was met, nor the entry of an order of approval under § 1805. See 50 U.S.C. § 1806(k)(2).[27]

(3) A "Significant Purpose" To Obtain Foreign Intelligence Information Is Sufficient to Support the Application of FISA's Standards to Surveillance Applications

Abu-Jihaad does not dispute the considerations prompting Congress's adoption of the "significant purpose" amendment. Rather, he argues that if FISA's probable cause standards are applied without a "primary" government purpose to obtain foreign intelligence information, the executive will be able to manipulate FISA to obtain surveillance warrants for criminal investigations without demonstrating the probable cause required by Title III for that purpose. Because we conclude that the required certification of "a significant purpose" to obtain foreign intelligence information adequately protects against this possibility, we reject Abu-Jihaad's constitutional challenge to this language.

As Congress and the courts have recognized, government investigations relating to national security frequently pursue more than one purpose. See United States v. Duggan, 743 F.2d at 78 (stating that, in enacting FISA, "Congress recognized that in many cases the

[27] Although some senators who voted for the PATRIOT Act thought it possible that courts might impose a constitutional requirement of "primary purpose," see In re Sealed Case, 310 F.3d at 737 (quoting remarks of Senator Leahy, 147 Cong. Rec. S11003 (Oct. 25, 2001), and Senator Edwards, 147 Cong. Rec. S10589 (Oct. 11, 2001)), for reasons stated in the next section of this opinion, we agree with the FISA Review Court that "a significant purpose" requirement is adequate to ensure that FISA standards are reasonably applied to the purpose for which they were identified.

concerns of the government with respect to foreign intelligence will overlap those with respect to law enforcement"); see also in re FISA Section 105B Directives, 551 F.3d at 1011 ("A surveillance with a foreign intelligence purpose often will have some ancillary criminal law purpose."). Indeed, multiple purposes may be inevitable given FISA's definition of "foreign intelligence information" and "agent of a foreign power" by reference to serious criminal conduct. See In re Sealed Case, 310 F.3d at 724 (observing that "foreign intelligence information" as defined in FISA "'can include evidence of certain crimes relating to sabotage, international terrorism, or clandestine intelligence activities'" (quoting H.R. Rep. No. 95-1283, at 49 (1978)) (emphasis omitted)); see also 50 U.S.C. § 1801(b) (defining "agent of foreign power" by reference to involvement in, inter alia, clandestine intelligence gathering, sabotage, and international terrorism). In such circumstances, intelligence and law enforcement purposes "'tend to merge,'" making it difficult to identify one as primary. See In re Sealed Case, 310 F.3d at 724-25 (quoting S. Rep. No. 95-701, at 10-11 (1978)). Indeed, as experience has taught, if the executive is required to certify that its "primary" purpose in conducting surveillance is to obtain foreign intelligence information, it may well have to exclude law enforcement officials from playing any part in the surveillance. Such a segregation of purposes makes no sense in terms of protecting national security. See id. at 727 ("[I]f one considers the actual ways in which the government would foil espionage or terrorism it becomes apparent that criminal prosecution analytically cannot be placed easily in a separate response category."). More important for our purposes, it is

not compelled by the Fourth Amendment.

For Fourth Amendment purposes, the critical question is not whether the executive can certify that obtaining foreign intelligence information is its "primary" purpose, but whether it can certify that it is a bona fide purpose of the surveillance. Thus, where the executive in good faith pursues both intelligence and law enforcement purposes, it may apply for surveillance authority under either FISA or Title III, provided it satisfies the particular warrant standards of the statute invoked. A Fourth Amendment concern would arise only if the executive, without a bona fide purpose to obtain foreign intelligence information, tried to secure a warrant under the standards identified in FISA as reasonable for that purpose.

We need not here decide at what point a purpose advanced by the executive might be so trivial as to preclude it from being pursued in good faith. Congress adequately safeguarded against that possibility in FISA by demanding certification of "a significant purpose" to obtain foreign intelligence information, rather than simply "a purpose" as originally requested by the executive. Moreover, the FISA Review Court, whose rulings bind the FISA Court in issuing surveillance warrants under the statute, has construed the significant purpose standard to require "that the government have a measurable foreign intelligence purpose, other than just criminal prosecution of even foreign intelligence crimes." Id. at 735.[28] Indeed, the FISA Review Court has ruled that the significant purpose

[28] Because In re Sealed Case, 310 F.3d 717, was decided in 2002, before the FISA orders here at issue here were entered, we can assume that its construction of the statute's provisions controlled the issuance of those orders.

requirement specifically "excludes from the purpose of gaining foreign intelligence information a sole objective of criminal prosecution," even for foreign intelligence crimes. Id.; see also id. at 736 (rejecting government's argument that "significant purpose" requirement allowed it to have primary objective of prosecuting foreign agent for non-foreign-intelligence crime, and noting that "the manifestation of such a purpose" would "disqualify an application").

The FISA Review Court has also plainly ruled that the government's certified purpose in seeking a FISA warrant is subject to judicial review. See id. at 735-36 (recognizing FISA Court's authority to seek more information pertaining to government's purpose). While "a significant purpose standard" eliminates "any justification for the FISA Court to balance the relative weight the government places on criminal prosecution," if the court determines that the government's sole objective is "merely to gain evidence of past criminal conduct – even foreign intelligence crimes – to punish the agent rather than halt ongoing espionage or terrorist activity, the application should be denied." Id. at 735. Thus, the FISA Review Court has ruled that to satisfy the significant purpose test, it must appear that "the government entertains a realistic option of dealing" with the target of the FISA surveillance "other than through criminal prosecution." Id.

We do not here decide which, if any, of these FISA Review Court conclusions are constitutionally compelled. We conclude simply that FISA's "significant purpose" requirement, so construed, is sufficient to ensure that the executive may only use FISA to

obtain a warrant when it is in good faith pursuing foreign intelligence gathering, the purpose for which that statute's warrant standards apply. The fact that the government may also be pursuing other purposes, including gathering evidence for criminal prosecution, compels no different conclusion.

Accordingly, we reject Abu-Jihaad's argument that FISA is unconstitutional because it does not require certification of a primary purpose to obtain foreign intelligence information. Rather, we hold that certification of a significant purpose to obtain foreign intelligence information, together with satisfaction of all other FISA requirements, is reasonable and, therefore, sufficient to support the issuance of a warrant under the Fourth Amendment.

2. FISA Was Lawfully Applied to This Case

Abu-Jihaad submits that, even if FISA is not unconstitutional on its face, his conviction must be vacated because the statute's conditions were not satisfied in securing some of the evidence supporting his conviction. Specifically, Abu-Jihaad contends that the government's application for a surveillance order (a) failed to satisfy the "significant purpose" requirement of 50 U.S.C. § 1804(a)(6)(B); (b) failed to demonstrate probable cause to believe that he was an agent of a foreign power or that his telephones were being used or about to be used by a foreign power or agent of such a power, see id. § 1804(a)(3)(A)-(B); (c) included "clearly erroneous" § 1804(a)(6) certifications; and (d) was based on false statements, requiring a hearing under Franks v. Delaware, 438 U.S. 154 (1978). Moreover,

he faults the district court for deciding these questions against him without affording him access to the FISA warrant application papers and an adversarial hearing.

a. The District Court Properly Denied Disclosure and a Hearing

In FISA, Congress expressly provided that where, as here, the Attorney General certifies that "disclosure [of FISA materials] or an adversary hearing would harm the national security of the United States," a district court must "review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted." 50 U.S.C. § 1806(f). While the district court retains authority to order disclosure of FISA materials "under appropriate security procedures and protective orders," it may do so "only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." Id. Where the court "determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure." Id. § 1806(g). Mindful of these provisions, we have concluded that disclosure of FISA materials "is the exception and ex parte, in camera determination is the rule." United States v. Stewart, 590 F.3d at 129 (internal quotation marks and brackets omitted).

Here the district court found that "review of the FISA materials in this case [was] relatively straightforward and not complex." United States v. Abu-Jihaad, 531 F. Supp. 2d 299, 310 (D. Conn. 2008). Further, while keeping "the requirements of the Constitution, the

statute, and Duggan fixed firmly in mind[,]" the district court determined that disclosure and an adversary hearing were unnecessary because its in camera, ex parte review permitted it to assess the legality of the challenged surveillance and the requirements of due process did not counsel otherwise. Id. at 311 & n.11. Upon our own review of the materials supporting the challenged FISA orders, we reach the same conclusions. Accordingly, we identify no denial of due process in the district court's decision not to order disclosure of FISA materials to the defendant, or to conduct a preliminary hearing to rule on Abu-Jihaad's challenge to FISA's implementation in this case.

b. The Government Satisfied FISA's Warrant Requirements, and There is No Basis in the Record for a *Franks* Hearing

In considering Abu-Jihaad's claims that the government failed to satisfy the significant purpose, probable cause, and certification requirements of FISA, and proffered false information warranting a Franks hearing, we have conducted a careful in camera review of the challenged FISA orders, the government's applications for those orders, and the classified materials submitted in support of those applications. We have similarly reviewed the government's classified Memorandum in Opposition to the Defendant's Motion for Suppression of FISA Evidence and Motion for Disclosure of FISA Applications, Orders and Related Materials and an Adversary Hearing; the classified declaration of Joseph Billy, Jr., Assistant Director of the Counterterrorism Division of the FBI; and the FBI's classified declaration regarding its compliance with minimization procedures applicable to the challenged orders. Like the district court, we conclude that there is no merit to any of Abu-

Jihaad's challenges to the government's compliance with FISA requirements in this case, nor any basis for a Franks hearing.

FISA warrant applications are subject to "minimal scrutiny by the courts," both upon initial presentation and subsequent challenge. United States v. Duggan, 743 F.2d at 77. Of course, even minimal scrutiny is not toothless. Cf. Wilson v. C.I.A., 586 F.3d 171, 185 (2d Cir. 2009) (observing in non-FISA context that "[d]eferential review" of classification challenge "does not equate to no review" (citing John Doe, Inc. v. Mukasey, 549 F.3d 861, 881 (2d Cir. 2008))). In reviewing a warrant application, the FISA Court properly considers whether (1) the application makes the probable cause showing required by FISA, i.e., that the target of the warrant is a foreign power or agent thereof and that the facilities or places to be searched or surveilled are being used or about to be used by a foreign power or its agent; (2) the application is otherwise complete and in the proper form; and (3) when the target is a United States person, the application's certifications are not "clearly erroneous." United States v. Duggan, 743 F.2d at 77. Further, as the FISA Review Court has now clarified, in deciding whether to grant a warrant application, the FISA Court may also request more information – including information as to purpose – as necessary to make these discrete determinations. See In re Sealed Case, 310 F.3d at 736 ("[I]f the FISA court has reason to doubt that the government has any real non-prosecutorial purpose in seeking foreign intelligence information it can demand further inquiry into the certifying officer's purpose."). In considering challenges to FISA Court orders, however, "the representations and

certifications submitted in support of an application for FISA surveillance should be presumed valid" by a reviewing court absent a showing sufficient to trigger a Franks hearing. United States v. Duggan, 743 F.2d at 77 n.6.

Although the established standard of judicial review applicable to FISA warrants is deferential, the government's detailed and complete submissions in this case would easily allow it to clear a higher standard of review. While we are necessarily circumspect in our discussion of these materials, like the district court, we observe that they "described at length the facts supporting the Government's assertion that there was probable cause to believe that the target of the FISA surveillance" – who was "described with particularity" – "was an agent of a foreign power," as well as "the basis for believing that the facilities at which electronic surveillance would occur [were] being used, or about to be used, by the target." United States v. Abu-Jihaad, 531 F. Supp. 2d at 313. Further, the application papers detailed facts "supporting the Government's certification that a significant purpose of the surveillance was to gather foreign intelligence information." Id.

This record convincingly satisfies FISA's purpose and probable cause requirements, and further reveals no clear error in the certifications by high-ranking executive officials. See id. at 312. We therefore reject Abu-Jihaad's conclusory claims to the contrary as without merit. Further, because nothing in the record before this court – which includes the full trial record – provides any basis to think that the FISA application contained any false statement, much less one made "knowingly and intentionally, or with reckless disregard for the truth,"

Franks v. Delaware, 438 U.S. at 155, we identify no error in the district court's decision not to hold a Franks hearing.

In sum, because we identify no constitutional infirmity in Congress's decision to allow FISA warrants to issue on certification of a "significant purpose" to obtain foreign intelligence information, and because we conclude that the record – without need for further disclosure or hearing – convincingly demonstrates that all FISA warrant requirements were satisfied in this case, we conclude that the district court correctly denied Abu-Jihaad's motion to suppress FISA-derived evidence.

B. The Evidentiary Challenges

Abu-Jihaad asserts that evidentiary errors deprived him of his due process right to a fair trial. Specifically, he submits that (1) recordings of telephone conversations in which he participated in 2006 were not relevant to the charged 2001 communication of national defense information, see Fed. R. Evid. 401, and, in any event, more prejudicial than probative, see Fed. R. Evid. 403; and (2) videos obtained from and materials available on Azzam's websites should also have been excluded under Rule 403. The district court ruled to the contrary in two detailed written decisions. See United States v. Abu-Jihaad, 553 F. Supp. 2d 121 (D. Conn. 2008) (ruling on videos and website materials); United States v. Abu-Jihaad, No. 07 Cr. 57, 2008 WL 282368 (D. Conn. Jan. 31, 2008) (ruling on 2006 recordings).

We review a district court's evidentiary rulings deferentially, mindful of its superior

position to assess relevancy and to weigh the probative value of evidence against its potential for unfair prejudice. See United States v. Royer, 549 F.3d 886, 901 (2d Cir. 2008). We will reverse an evidentiary ruling only for "abuse of discretion," see United States v. Quinones, 511 F.3d 289, 307 (2d Cir. 2007), which we will identify only if the ruling was "arbitrary and irrational," United States v. Dhinsa, 243 F.3d 635, 649 (2d Cir. 2001) (internal quotation marks omitted). That is plainly not this case.

1. The 2006 Recordings

A review of the recorded conversations confirms the district court findings that therein Abu-Jihaad demonstrated his familiarity with Azzam as an organization sympathetic to jihad and admitted his own correspondence with Azzam through its websites, specifically in an email discussing the bombing of the U.S.S. Cole. See United States v. Abu-Jihaad, 2008 WL 282368, at *4. In the conversations, Abu-Jihaad further demonstrated an obsession with secrecy in discussing matters related to jihad. Not only did he routinely employ code in discussing confederates and objectives, he discussed his inability to provide a purported jihad sympathizer with current military intelligence in coded terms that supported an inference that he had provided such intelligence in the past. See id. at *5-6. Although these conversations made no mention of the charged disclosure of the Battlegroup Document and, in fact, took place more than four years after that charged crime, they were undoubtedly relevant to a jury's assessment of Abu-Jihaad's guilt.

To be relevant, evidence need not be sufficient by itself to prove a fact in issue, much

less to prove it beyond a reasonable doubt. See Contemporary Mission, Inc. v. Famous Music Corp., 557 F.2d 918, 927 (2d Cir. 1977) ("Evidence need not be conclusive in order to be relevant."). Rather, evidence is "relevant" if it has "any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence." Fed. R. Evid. 401; see United States v. Schultz, 333 F.3d 393, 416 (2d Cir. 2003) ("Nonconclusive evidence should still be admitted if it makes a proposition more probable than not." (internal quotation marks omitted)).

Abu-Jihaad's discussions of Azzam, its websites, and his email communications with that organization were relevant because they linked him to the recipient of the Battlegroup Document. This fact made it more probable that, among the discrete group of persons with knowledge of the classified information at issue, Abu-Jihaad was the source of the unauthorized disclosure to Azzam. Although Abu-Jihaad endeavored to reduce this likelihood by offering evidence that some transit plan information was more widely available than the Navy maintained, see infra at 59-60, such evidence would have affected only the weight, not the admissibility, of the recorded conversations. See United States v. Schultz, 333 F.3d at 416 (observing that "factors which make evidence less than conclusive affect only weight, not admissibility" (internal quotation marks omitted)).

Similarly, the recordings demonstrating Abu-Jihaad's keen concern with secrecy were relevant both generally in demonstrating consciousness of guilt and specifically in explaining why there was no evidence on Azzam websites about transmittal of the Battlegroup

Document or the information contained therein. As for Abu-Jihaad's recorded discussion of why he could not provide current military intelligence – "I ain't been working ah in, in the field of making meals and or, you know . . . [i]n a, in a long time. I've been out of that for, ah, over ah, quatro years you know," Trial Tr. at 989-90; Gov't Ex. 141k at 7 – the statement permitted an inference that, four years earlier, Abu-Jihaad had been engaged in "making meals," i.e., providing military intelligence, an admission highly probative of his commission of the charged crime. That the statement might be construed more innocently was a matter properly addressed through cross-examination and argument to the jury, not a ground for excluding the evidence as irrelevant.

Rule 403 warrants no different conclusion. As we observed in United States v. LaFlam, 369 F.3d 153 (2d Cir. 2004), when we review a district court's evaluation of evidence under Rule 403, we "generally maximize its probative value and minimize its prejudicial effect," id. at 155 (internal quotation marks and brackets omitted). Applying this standard, we conclude that the recorded discussions were both highly probative of the charged crime and, to the extent they referenced uncharged contemporaneous support for jihad, no more inflammatory than the charges alleged in the indictment. In any event, the district court properly minimized the risk of unfair prejudice through limiting instructions. See United States v. Mercado, 573 F.3d 138, 142 (2d Cir. 2009) (upholding Rule 403 determination where challenged evidence "not especially worse or shocking than the transactions charged" and where district court "gave several careful instructions to the jury

regarding what inferences it could draw from the admitted evidence").

The district court instructed the jury that (a) "Abu-Jihaad [was] not . . . charged with anything based on the conversations . . . from 2006," (b) "the events that form[ed] the basis of the charges against . . . Abu-Jihaad in this case occurred in 2001, not 2006," and (c) the jury was "not to speculate about what was the nature of the investigation" involving Shareef and the confidential informant or "whether or if any charges resulted from that investigation." Trial Tr. at 992. Abu-Jihaad does not challenge the adequacy of these instructions. Thus, his contention that the 2006 recordings permitted the jury to speculate about Shareef's plans reduces to a challenge to the presumption that jurors follow the instructions they are given. See United States v. Downing, 297 F.3d 52, 59 (2d Cir. 2002) ("Absent evidence to the contrary, we must presume that juries understand and abide by a district court's limiting instructions."). Because Abu-Jihaad points to nothing in the record to undermine this presumption, we identify no merit in his argument, and we conclude that the district court acted well within its discretion in admitting the 2006 recordings.

2. Azzam Website Materials

We reach the same conclusion with respect to the admitted Azzam website materials, which consisted of (a) excerpts from three videos purchased by Abu-Jihaad from Azzam, and (b) other materials marketed and/or posted on Azzam's webstites. Abu-Jihaad concedes the relevancy of these materials to an understanding of Azzam's operations and to his own mens rea. Nevertheless, he contends that the evidence should have been excluded under Rule 403.

We are not persuaded.

a. Video Evidence

With respect to the videos, which we briefly describe supra at 12-13 & n.12, the district court determined that the pro-jihadist contents of the videos were relevant to understanding Abu-Jihaad's motive and intent in communicating information that could have resulted in the destruction of the very ship on which he served. See United States v. Abu-Jihaad, 553 F. Supp. 2d at 127-28. At the same time, the district court was conscientious in ensuring against unfair prejudice. See United States v. Salameh, 152 F.3d 88, 110 (2d Cir. 1998). It reviewed the films in their entirety before approving only selected excerpts for display to the jury. Although these excerpts included depictions of violence, as was necessary not to distort the sense of the films as a whole, the depictions were limited and, as the district court accurately observed, less gruesome than many seen on "nightly news dispatches from Baghdad." United States v. Abu-Jihaad, 553 F. Supp. 2d at 128.[29]

We identify no error, let alone arbitrary or irrational error, in the decision of admissibility under these circumstances. See United States v. Salameh, 152 F.3d at 110-11 (holding that where video depicting embassy bombing and instructions for making explosive

[29] Thus, the government was permitted to show only one minute of a nine minute segment of the bloody bodies of jihad martyrs. It was required to redact scenes depicting a headless body and one with a badly severed neck. See United States v. Abu-Jihaad, 553 F. Supp. 2d at 128. We express no opinion as to whether such scenes could be displayed to a jury without violating a defendant's right to a fair trial. We cite their redaction only to illustrate the care taken by the district court to avoid unfair prejudice.

devices was relevant to motive and nature of conspiratorial agreement, district court did not abuse its discretion in concluding that probative value of evidence outweighed any unfair prejudice). Moreover, any danger of unfair prejudice was here again minimized by the district court's limiting instructions, see United States v. Bermudez, 529 F.3d 158, 163 (2d Cir. 2008), which we presume the jury followed, see United States v. Downing, 297 F.3d at 59.[30] Accordingly, we conclude that the district court acted within its discretion in allowing the jury to view the challenged video evidence.

b. Website Materials

The district court also allowed the jury to view various materials, including Osama bin Laden's 1996 fatwa against the United States, that were marketed or posted on Azzam's websites in or around 2001. The government could not prove that Abu-Jihaad saw a particular posting, only that he visited the site during times when the postings were available. See United States v. Abu-Jihaad, 553 F. Supp. 2d at 128-29. The court acknowledged that such materials had the potential to "inflame a juror's passions." Id. at 129. Nevertheless, it concluded that the risk of such prejudice did not outweigh the probative value of the materials to the jury's assessment of Abu-Jihaad's intent and motive in communicating with

[30] The district court charged the jury that the videos could be considered only in determining the knowledge and intent with which Abu-Jihaad undertook any actions proved against him. See Trial Tr. at 259-60, 401. Moreover, the court instructed the jury to consider the video evidence "dispassionately, and even if there's material that you find personally distasteful, you can't let your personal opinions, your fears, your biases, to enter into your consideration." Id. at 401.

Azzam. In reaching this conclusion, the court emphasized that it had gone to "extraordinary lengths" to select jurors who would not let passion or bias infect their consideration of evidence and who would conscientiously follow appropriate limiting instructions. Id. On this record, we identify no abuse of discretion in admission of the Azzam website materials.

C. The Sufficiency Challenge

Abu-Jihaad argues that the district court erred in denying his motion for acquittal on the 18 U.S.C. § 793(d) count of conviction because the trial evidence was insufficient to prove guilt. See Fed. R. Crim. P. 29. The rule of constitutional sufficiency derives from the Due Process Clause and instructs that no conviction may be obtained "except upon proof beyond a reasonable doubt of every fact necessary to constitute the crime . . . charged." In re Winship, 397 U.S. 358, 364 (1970); see also Jackson v. Virginia, 443 U.S. 307, 318-19 (1979). While we review de novo the denial of a Rule 29 sufficiency challenge, see United States v. Pizzonia, 577 F.3d 455, 462 (2d Cir. 2009), we apply the same deferential standard as the district court in assessing the trial evidence, i.e., we view that evidence in the light most favorable to the government, assuming that the jury resolved all questions of witness credibility and competing inferences in favor of the prosecution, see United States v. Burden, 600 F.3d 204, 214 (2d Cir. 2010); United States v. Payne, 591 F.3d 46, 60 (2d Cir. 2010). A defendant mounting a sufficiency challenge thus "bears a very heavy burden," United States v. Desena, 287 F.3d 170, 177 (2d Cir. 2002), because a court must uphold a jury verdict so long as "'any rational trier of fact could have found the essential elements of the

crime beyond a reasonable doubt,'" United States v. Stewart, 590 F.3d at 109 (quoting Jackson v. Virginia, 443 U.S. at 319 (emphasis in original)). That is certainly this case.

The thrust of Abu-Jihaad's sufficiency challenge is that the government's case rested entirely on circumstantial evidence. Direct evidence, however, is not constitutionally required to support a conviction. The law is well established that the government may secure conviction based solely on circumstantial evidence, provided it is sufficient to prove the elements of the charged crime beyond a reasonable doubt. See United States v. Lorenzo, 534 F.3d 153, 159 (2d Cir. 2008). To convict Abu-Jihaad of the § 793(d) crime with which he was charged, the government was required to prove beyond a reasonable doubt that he (1) lawfully had possession of, access to, control over, or was entrusted with information relating to the national defense; (2) had reason to believe that such information could be used to the injury of the United States or to the advantage of any foreign nation; (3) willfully communicated, delivered, transmitted, or caused to be communicated, delivered, or transmitted such information; and (4) did so to a person not entitled to receive it. See 18 U.S.C. § 793(d); see also United States v. Abu-Jihaad, 600 F. Supp. 2d at 384 (quoting jury charge).[31]

---

[31] Title 18 U.S.C. § 793(d) states:

> Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the

Abu-Jihaad does not – and cannot – challenge the sufficiency of the evidence to establish the first, second, and fourth elements of the crime. The trial evidence convincingly showed that, as a member of the U.S.S. Benfold's navigation division with a "secret" security clearance, Abu-Jihaad had access to the Constellation battlegroup's transit plan and the classified information contained therein. Further, because the transit plan was classified as "confidential" and contained information about the anticipated movements of Navy ships into areas of heightened vulnerability to attack, there can be no question that this information related to the national defense. See Gorin v. United States, 312 U.S. 19, 28 (1941) (construing phrase "national defense" in context of Espionage Act as "generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness" (internal quotation marks omitted)); United States v. Heine, 151 F.2d 813, 815-17 (2d Cir. 1945) (L. Hand, J.) (construing "information relating to the national defense" to include only information that is closely held).[32] Moreover, given

> national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it . . . [s]hall be fined under this title or imprisoned not more than ten years, or both.

[32] Although Abu-Jihaad argues that information in the Battlegroup Document was publicly available, the evidence he offered in support of that claim showed only that some general information regarding the Constellation battlegroup's transit schedule had entered

the classified nature of the information and Abu-Jihaad's demonstrated understanding in his Cole email of the impact of an attack on a United States warship, a rational juror could certainly conclude that the defendant had reason to believe that information regarding the navigational route and schedule to be followed by the Constellation battlegroup could be used to injure the United States. Finally, there is no question that neither Babar Ahmad, from whose residence the Battlegroup Document was recovered, nor Syed Talha Ahsan, who appeared to have created the file containing that document, nor any other person associated with Azzam, was authorized to receive classified United States military information.

Thus, Abu-Jihaad's sufficiency challenge is reasonably understood to focus on the third element of the crime. He submits that the trial evidence was insufficient to permit any rational jury to find beyond a reasonable doubt that he was the person who willfully made the charged disclosure of national defense information. Although the district court observed that this challenge was not "insubstantial" given that the supporting evidence for this element was largely circumstantial, see United States v. Abu-Jihaad, 600 F. Supp. 2d at 365, upon careful review of the record, it concluded that the evidence was sufficient to permit the jury to find the third element proved beyond a reasonable doubt. Upon our own review of the record, we reach the same conclusion. From circumstances indicating that (1) the

---

the public domain prior to the date of deployment. See infra at 59-60. The public information adduced by Abu-Jihaad at trial did not preclude any rational jury from concluding that the transit plan with which he was entrusted, and the Battlegroup Document derived therefrom, contained information relating to the national defense.

information in the Battlegroup Document communicated to Azzam came from a Navy insider, (2) Abu-Jihaad was an insider with access to that information and the only identified member of the Navy who communicated support for jihad to Azzam in the relevant time period, and (3) Abu-Jihaad admitted disclosing military intelligence while in the Navy, a reasonable jury could conclude beyond a reasonable doubt that Abu-Jihaad was, in fact, the person who had willfully disclosed the classified information in the Battlegroup Document to Azzam.

1. The Information in the Battlegroup Document Came from a Navy Insider

The contents of the Battlegroup Document, specifically, its identification of significant dates referenced in the classified transit plan – notably March 20, 2001, for an ammunition stop in Hawaii; April 6, 2001, for a port call in Sydney; and April 29, 2001, for passage through the Strait of Hormuz (in fact, the date for crossing the CHOP point) – strongly supported an inference that the source of the information contained therein had to have been a Navy insider. In urging otherwise, Abu-Jihaad relies on arguments that he unsuccessfully made to the jury: that the Battlegroup Document contained so much publicly available information and so many errors that it could just as easily, if not more likely, have been transmitted by someone outside the Navy. The jury's rejection of this argument was hardly irrational.

To the extent the defense adduced evidence in the public domain about movements of the Constellation battlegroup, it failed to demonstrate that the majority of that information

was available prior to the battlegroup's March 15, 2001 deployment, as would have been necessary for publicly available information to have informed creation of the Battlegroup Document. The information that was shown to have been publicly available before deployment failed to provide sufficient facts from which to compile the Battlegroup Document. Specifically, a February 11, 2001 post to a Massachusetts Institute of Technology alumni website stated only that a carrier pilot would be deploying for six months aboard the U.S.S. Constellation, which was expected to make port calls in Sydney, Perth, Bahrain, and Dubai. We need not here assess the relative indiscretion of such a post. We note simply that it did not provide specific dates for the identified ports of call, as contained in the Battlegroup Document. Nor did it mention Hawaii as a port of call, a fact included only in the final transit plan. Similarly, although a pre-deployment press release from the Canadian Navy indicated that the Constellation battlegroup would arrive in the Arabian Gulf in early May 2001, and a February 2001 article about the Tarawa Amphibious Readiness Group identified Phuket, Thailand, as a favorite port of call for the Navy and the Marines, neither document provided any specific information about the Constellation battlegroup's expected ports of call, let alone the dates on which any ships would reach those ports.

Similarly unavailing is Abu-Jihaad's reliance on errors in the Battlegroup Document to argue that the source of its information could not have been a Navy insider. To the extent the errors involve misspelling of Navy terms, the jury would have seen that Navy insider Abu-Jihaad routinely misspelled ordinary words in his emails with Azzam. Insofar as

defendant points to the Battlegroup Document's misidentification of April 29, 2001, as the date for transit through the Strait of Hormuz (when in fact it was the date for crossing the CHOP point) and March as a tax-free month (when in fact it was April), a reasonable jury could have concluded that the errors were either inadvertent, introduced after the information was originally conveyed, or reflective of a Navy insider conveying information outside his particular area of responsibility. Indeed, a jury might reasonably have rejected the coincidence of anyone other than an insider selecting the same date (April 29, 2001) for transiting the Strait of Hormuz as had been emphasized in each iteration of the transit plan for crossing the CHOP point, particularly as the latter event would take place only a short time before the ships entered the Strait of Hormuz, an easily identified natural geographic reference compared to the CHOP point, which was defined only by degrees of latitude and longitude. Moreover, a jury was entitled to consider that the Battlegroup Document concluded with the instruction: "Please destroy message." Gov't Ex. 1. A person transmitting publicly available information would have less reason to include such an instruction than a Navy insider transmitting classified information.

2. Abu-Jihaad's Access to the Disclosed Information and Ties to Azzam

That Abu-Jihaad was the insider who transmitted classified information about the Constellation battlegroup's transit plan was established, in part, by evidence of his opportunity and motive to do so. Abu-Jihaad does not seriously dispute that, as a signalman with a secret-level security clearance, he had access to the transit plan and, thus, the

opportunity to transmit it to an unauthorized person. See United States v. Abu-Jihaad, 600 F. Supp. 2d at 377 (referencing evidence that Abu-Jihaad "regularly worked on the bridge where . . . the ship's paper charts and classified transit plans were stored"). Nor does he dispute that he frequently communicated with Azzam, the unauthorized recipient of the classified information in 2001, or that the contents of his communications revealed a motive to transmit classified information, i.e., his support for jihad, even when directed against his own country.

Instead, Abu-Jihaad submits that any inference that he transmitted classified information to Azzam was undermined by his open display of jihadist sympathies in the Navy, as evidenced by his sharing Azzam videos with shipmates and his use of a Navy-monitored email account to communicate with Azzam. While Abu-Jihaad was free to make this argument to the jury, it was hardly compelled to accept it and to return a verdict of not guilty. The jury could have determined that if Abu-Jihaad used his military account to convey national defense information, he did so prior to the battlegroup's March 15, 2001 deployment and, thus, at a time when his Navy email was not being monitored. Alternatively, the jury could have found that Abu-Jihaad likely used his personal email account to transmit classified information. That, after all, was the account he used to send his Cole email to Azzam praising the murderous bombing of a Navy ship as a "martyrdom operation." See Gov't Ex. 19.

In urging otherwise, Abu-Jihaad observes that in the Cole email, sent in July 2001, he

introduced himself as a United States sailor, an unnecessary action if he had previously disclosed military intelligence to Azzam. The Cole email, however, was sent to an Azzam email account specifically designated for the general public to send emails of support. A rational jury might well have concluded that Abu-Jihaad sent the classified information to a different Azzam email address, with or without introducing himself.

In sum, even if the email evidence could have supported inferences more favorable to Abu-Jihaad, it was nevertheless sufficient to support a reasonable inference that Abu-Jihaad was the only person shown to have had both the opportunity and motive to transmit the classified transit plan information to Azzam. See United States v. Burden, 600 F.3d at 226 (reiterating established rule that it is for jury to choose among competing inferences supported by evidence).

3. Abu-Jihaad's Admitted Disclosure of Navy Intelligence

In addition to evidence establishing Abu-Jihaad's opportunity and motive to disclose classified information, the jury heard recorded statements in which Abu-Jihaad effectively admitted to having actually done so. In a series of conversations intercepted in 2006, which we detail in our discussion of the facts, see supra at 15-19, Abu-Jihaad repeatedly discussed providing Shareef, a suspected terrorist sympathizer, with "meals." A confidential informant who participated in some of the conversations testified at trial that "meals" was a code for military intelligence. Thus, while generally promising Shareef support, Abu-Jihaad explained that he had been out of the Navy too long to have any current intelligence to

convey: "I haven't been on that job, so I don't – you know what I'm saying, I haven't been there . . . to see . . . what the fresh meal is." Gov't Ex. 141h at 1. Abu-Jihaad nevertheless encouraged Shareef to speak with "the Mexican," identified at trial as Miguel Colon, who had been discharged from the Navy only two months earlier: "[H]e can give you a fresh meal 'cuz . . . he just finished his job, there, less than a month ago . . . ." Id. at 1-2. Then, in a conversation that same day with Colon about Shareef's desire for intelligence, Abu-Jihaad made the statement that the government argued acknowledged his past transmittal of intelligence information: "I don't know how to get him no hot meal . . . . I ain't been working uh, in, in, in the field of making meals and or, you know . . . in a long time. I've been out of that for uh, over uh, quatro years you know." Gov't Ex. 141k at 7.

Although Abu-Jihaad suggests that the statement only indicated that he was not in a position to secure current intelligence because he had been out of the Navy for four years, a reasonable jury could have construed the statement as an admission of past intelligence disclosures. Abu-Jihaad did not, after all, state simply that he had never worked "in the field of making meals," i.e., providing military intelligence. Rather, he stated that he "ain't been working uh, in, in, in the field of making meals and or, you know . . . in a long time." Implicit in a statement that one has not done something "in a long time" is an admission to having done that thing at some time in the past, in Abu-Jihaad's case, "working . . . in the field of making meals," i.e., providing military intelligence, some four years ago when he was in the Navy and held a security clearance to access certain classified information.

While Abu-Jihaad's implicit admission is general, making no specific reference to the Battlegroup Document, on a sufficiency challenge, we review pieces of evidence not in isolation, but in conjunction. See United States v. Rigas, 490 F.3d 208, 230 (2d Cir. 2007); United States v. Miller, 116 F.3d 641, 676 (2d Cir. 1997). Here the totality of the evidence permitted the jury to find, inter alia, that: classified information about Navy operations was transmitted to Azzam, an organization sympathetic to violent jihad; the source of the disclosed classified information was a Navy insider; Abu-Jihaad was a Navy insider with access to the classified information at issue; defendant was in regular communication with Azzam at and about the time relevant to the charged disclosure; although some of Abu-Jihaad's communications had been deleted, those that were retrieved revealed his strong support for jihad, even when directed against his own country; no other member of the United States military had such a record of communication with Azzam; and Abu-Jihaad essentially admitted in recorded conversations to disclosing classified information during his service in the Navy. These findings, in turn, were sufficient to support a finding beyond a reasonable doubt that Abu-Jihaad was the person who communicated national defense information pertaining to the 2001 transit plan for the Constellation battlegroup to persons at Azzam in violation of 18 U.S.C. § 793(d). Accordingly, we conclude that Abu-Jihaad's challenge to the sufficiency of the evidence supporting his conviction is without merit.

E. CIPA Protective Orders

In his final challenge, Abu-Jihaad contends that the district court erred not only in

granting the government's motions for protective orders pursuant to Section 4 of the Classified Information Procedures Act ("CIPA"), 18 U.S.C. app. 3, §§ 1-16, but also in considering ex parte whether the classified materials – submitted and reviewed in camera – were discoverable. The district court set forth its reasons for issuing the challenged orders in two opinions. See United States v. Abu-Jihaad, No. 07 Cr. 57, 2008 WL 346121 (D. Conn. Feb. 4, 2008); United States v. Abu-Jihaad, No. 07 Cr. 57, 2008 WL 596200 (D. Conn. Feb. 22, 2008). Nevertheless, because neither Abu-Jihaad nor his counsel has had access to the government's submissions or the transcripts of the ex parte conferences, all of which have been maintained under seal, defendant submits that he "is in no position to present factual arguments that th[e] procedure [adopted by the district court] resulted in any prejudice." Appellant's Br. at 63. His CIPA challenge can thus be understood as a general request for this court to examine the sealed records and to assess the propriety of the district court's decision to grant protective orders.

We review for abuse of discretion a district court's decision to issue a protective order pursuant to Section 4 of CIPA, including its determination whether evidence is helpful or material to the defense and whether unclassified summaries or admissions are properly substituted for classified information. See United States v. Stewart, 590 F.3d at 131; United States v. Aref, 533 F.3d 72, 80 (2d Cir. 2008). We detect no such abuse here.

CIPA, which establishes certain procedures for the handling of classified information in criminal cases, is designed "to protect[] and restrict[] the discovery of classified

information in a way that does not impair the defendant's right to a fair trial." United States v. Aref, 533 F.3d at 78 (alterations in original; internal quotation marks omitted); see also United States v. Pappas, 94 F.3d 795, 799 (2d Cir. 1996) (observing that purpose of CIPA is to "establish procedures to harmonize a defendant's right to obtain and present exculpatory material upon his trial and the government's right to protect classified material in the national interest" (internal quotation marks omitted)). CIPA defines "[c]lassified information" as "any information or material that has been determined by the United States Government pursuant to an Executive order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security." 18 U.S.C. app. 3, § 1(a). In regulating the discovery of such information, Section 4 of CIPA instructs as follows:

> The court, upon a sufficient showing, may authorize the United States to delete specified items of classified information from documents to be made available to the defendant through discovery under the Federal Rules of Criminal Procedure, to substitute a summary of the information for such classified documents, or to substitute a statement admitting relevant facts that the classified information would tend to prove. The court may permit the United States to make a request for such authorization in the form of a written statement to be inspected by the court alone. If the court enters an order granting relief following such an ex parte showing, the entire text of the statement of the United States shall be sealed and preserved in the records of the court to be made available to the appellate court in the event of an appeal.

Id. app. 3, § 4. As we have recently observed, "[t]his section clarifies district courts' power under Federal Rule of Criminal Procedure 16(d)(1) to issue protective orders denying or restricting discovery for good cause, which includes information vital to the national security." United States v. Stewart, 590 F.3d at 130 (internal quotation marks omitted).

To be clear, CIPA does not confer on the government a privilege to refrain from disclosing classified information; it merely presupposes one. See id. The privilege it presupposes has its origins in the common-law privilege against disclosure of state secrets, see id.; United States v. Aref, 533 F.3d at 78, which "allows the government to withhold information from discovery when disclosure would be inimical to national security," Zuckerbraun v. Gen. Dynamics Corp., 935 F.2d 544, 546 (2d Cir. 1991). Although applicable in criminal cases, the state-secrets privilege must – under some circumstances – "give way . . . to a criminal defendant's right to present a meaningful defense." United States v. Stewart, 590 F.3d at 131 (internal quotation marks omitted). In determining when a defendant's right to present a defense displaces the state-secrets privilege, we apply the test announced in Roviaro v. United States, 353 U.S. 53 (1957), asking first, "whether the material in dispute is discoverable, and if so, whether the state-secrets privilege applies"; and second, if the privilege applies, "whether the information is helpful or material to the defense, i.e., useful to counter the government's case or to bolster a defense," United States v. Stewart, 590 F.3d at 131 (internal quotation marks omitted) (citing Roviaro).[33] For purposes of this test, the state-secrets privilege applies if "(1) there is a reasonable danger

[33] Information that is helpful or material to the defense "need not rise to the level that would trigger the Government's obligation under Brady v. Maryland, 373 U.S. 83 (1963), to disclose exculpatory information." United States v. Aref, 533 F.3d at 80 (citation omitted); see also United States v. Mejia, 448 F.3d 436, 457 (D.C. Cir. 2006) (observing that, for purposes of CIPA, "information can be helpful without being 'favorable' in the Brady sense").

that compulsion of the evidence will expose . . . matters which, in the interest of national security, should not be divulged, and (2) the privilege is lodged by the head of the department which has control over the matter, after actual personal consideration by that officer." United States v. Aref, 533 F.3d at 80 (ellipsis in original; internal quotation marks omitted).

1. The Government Adequately Established that the State-Secrets Privilege Applies

Having carefully reviewed the classified materials that are the subject of the challenged protective orders, we reach the same conclusion as the district court: that the government has demonstrated a reasonable danger that disclosure would jeopardize national security. Again, our discussion of the classified information is necessarily circumspect. Nevertheless, we conclude that the affidavits submitted by government officials satisfactorily identify specific facts that (a) render the materials here at issue classified and (b) support the conclusion that disclosure of those materials would pose a risk to national security.[34]

[34] Since the district court's challenged decisions in this case, we have held that representations about the security risks posed by disclosure must be made by the "head of the department which has control over the matter, after actual personal consideration by that officer." United States v. Aref, 533 F.3d at 80 (internal quotation marks omitted). To the extent that was not done here, we conclude, as we have in other cases, that there would be little gained by remanding the case solely to have the appropriate department head reassert the state-secrets privilege. See id.; United States v. Stewart, 590 F.3d at 132. This is not to trivialize the need for a formal claim of privilege "lodged by the head of the [relevant] department." United States v. Aref, 533 F.3d at 80 (internal quotation marks omitted). Indeed, "[w]e expect that, in light of the holding in Aref, we will not need to address this issue in appeals from future prosecutions in which the state-secrets privilege is invoked as the government is now well-informed of this obligation." United States v. Stewart, 590 F.3d at 132.

2. Abu-Jihaad Was Not Denied Information Helpful or Material to His Defense

We further conclude that the challenged protective orders did not deny Abu-Jihaad evidence that was either helpful or material to his defense. Although this court had not yet issued its decision in United States v. Aref, at the time the district court considered this question, that court did rely on a test, similar to that announced in Aref, identified by one of our sister circuits. See United States v. Abu-Jihaad, 2008 WL 346121, at *3-4 (citing United States v. Yunis, 867 F.2d 617, 622-25 (D.C. Cir. 1989)); United States v. Abu-Jihaad, 2008 WL 596200, at *1 (referring to standards governing discovery of classified information under CIPA set forth in prior CIPA ruling).[35] Applying that test, the district court concluded that none of the materials at issue in the government's first motion for a protective order were discoverable under Brady v. Maryland, 373 U.S. 83 (1963), Giglio v. United States, 405 U.S. 150 (1972), or Rule 16 of the Federal Rules of Criminal Procedure.[36] In particular, it noted that (a) "[m]ost of the information ha[d] nothing whatsoever to do with any issue in th[e] case or any criminal activity at all"; (b) none of the information could be deemed "helpful

[35] In United States v. Yunis, 867 F.2d at 622, the D.C. Circuit employed a "relevant and helpful" standard for determining whether classified information may be withheld under CIPA. In explaining the standard, the court held that "classified information is not discoverable on a mere showing of theoretical relevance," but only where relevant information "is at least helpful to the defense of the accused." Id. (internal quotation marks and brackets omitted).

[36] Insofar as the standard applied by the district court differed in any respect from that announced in United States v. Aref, 533 F.3d at 80, we identify no material difference given the facts of this case.

or beneficial to the defense," let alone exculpatory or impeaching; and (c) because Abu-Jihaad already had knowledge and/or possession of much of the information, its production would have been duplicative. United States v. Abu-Jihaad, 2008 WL 346121, at *5.

While the district court concluded that four of the six categories of information at issue in the government's second motion for a protective order were either undiscoverable or not "helpful or favorable to the defense," it determined that the remaining two categories contained discoverable information. United States v. Abu-Jihaad, 2008 WL 596200, at *2-4. Nevertheless, because one of the categories was cumulative of information already provided to Abu-Jihaad in the course of discovery, the district court determined that the government had no obligation to disclose such information. See id. at *3. As for the second category, the district court found the government's disclosure obligation satisfied by its production of various letters, FBI reports, and other discovery to the defense. See id. at *2-3.

Upon our own in camera review of the underlying materials and the sealed records preserved for appeal, including a detailed comparison of original discoverable documents with the unclassified summaries approved by the district court, we conclude that the district court's rulings with respect to the discoverable nature of the classified materials and the government's compliance with any extant discovery obligations manifest no abuse of discretion. Indeed, we commend the district court's careful discharge of its CIPA obligations, particularly its effective protection of Abu-Jihaad's rights despite the defense's limited ability to participate in the CIPA proceedings.

3. The District Court Properly Considered the Government's Motions for Protective Orders *Ex Parte*

Insofar as Abu-Jihaad faults the district court for entertaining the government's motions for protective orders ex parte, his argument is unconvincing. Abu-Jihaad does not dispute that Section 4 of CIPA and Rule 16(d)(1) of the Federal Rules of Criminal Procedure both authorize ex parte proceedings. Accordingly, his contention that such submissions are improper "[a]bsent a showing of exceptional circumstances," Appellant's Br. at 63, amounts to a challenge to the district court's exercise of discretion to proceed ex parte. The argument fails in light of our decision in United States v. Aref, in which we recognized that where the government moves to withhold classified information from the defense, "an adversary hearing with defense knowledge would defeat the very purpose of the discovery rules." 533 F.3d at 81 (internal quotation marks omitted). In such circumstances, a district court's decision to conduct ex parte hearings manifests no abuse of discretion. See id.; see also United States v. Stewart, 590 F.3d at 132 (identifying no error in district court's ex parte, in camera review of materials subject to CIPA motion because such a "method for protection of classified material is necessary," and CIPA procedures "have been established by Congress and held to be constitutional"); United States v. Klimavicius-Viloria, 144 F.3d 1249, 1261 (9th Cir. 1998) (concluding that while "[e]x parte hearings are generally disfavored," in a case involving classified documents, "ex parte, in camera hearings in which government counsel participates to the exclusion of defense counsel are part of the process that the district court may use in order to decide the relevancy of the information").

In sum, because we conclude that the government's submissions fully support the district court's entry of the challenged CIPA orders, that the district court acted well within its discretion in reviewing those submissions ex parte and in camera, and that the orders did not deny Abu-Jihaad any information helpful or material to his defense, we identify no basis in CIPA for vacating the conviction.

III. Conclusion

To summarize, we conclude that:

1. Evidence obtained pursuant to FISA warrants was properly admitted into evidence against defendant because FISA was not rendered unconstitutional by a PATRIOT Act amendment that allows surveillance warrants to issue upon certification by the executive of a "significant" rather than "primary" purpose to obtain foreign intelligence information. Such a certification, together with FISA's other requirements, strikes a reasonable balance between the government's interest in obtaining foreign intelligence information and the protection of individuals' Fourth Amendment rights.

2. Inculpatory evidence obtained pursuant to FISA warrants was properly admitted into evidence against defendant because all FISA requirements were complied with in this case, and due process did not demand disclosure of FISA applications to defendant or an adversarial hearing.

3. The district court acted within its discretion in admitting into evidence (a) recorded telephone conversations from 2006 in which defendant participated, (b) excerpts of three

videos purchased from Azzam by defendant, and (c) other materials marketed and/or posted on the Azzam websites in or around 2001.

4. The trial evidence was sufficient to support defendant's conviction for disclosing national defense information to persons not entitled to receive it in violation of 18 U.S.C. § 793(d).

5. The district court acted within its discretion in granting government motions for protective orders pursuant to Section 4 of CIPA.

Accordingly, the judgment of conviction is AFFIRMED.