UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

THOMAS WILNER, *et al.*,	)	
Plaintiffs,	)	Hon. Judge Cote
v.	)	1:07-cv-3883-DLC
NATIONAL SECURITY AGENCY, *et al.*,	)	
Defendants.	)	

MEMORANDUM IN SUPPORT OF DEFENDANTS' PARTIAL MOTION FOR SUMMARY JUDGMENT REGARDING THE GLOMAR RESPONSE

JEFFREY S. BUCHOLTZ
Acting Assistant Attorney General

JOSEPH H. HUNT
Director, Federal Programs Branch

ELIZABETH A. SHAPIRO
Assistant Director, Federal Programs Branch

ALEXANDER K. HAAS (CA# 220932)
Trial Attorney
Federal Programs Branch, Civil Division
United States Department of Justice
P.O. Box 883, 20 Massachusetts Ave., N.W.
Washington, D.C. 20044
Tel: (202) 305-9334 — Fax: (202) 305-3138
Email: alexander.haas@usdoj.gov

TABLE OF CONTENTS

PAGE

TABLE OF AUTHORITIES

CASES **PAGE(S)**

STATUTES , ORDERS, & PUBLIC LAWS

INTRODUCTION

Plaintiffs, lawyers who assert that they represent or have represented Guantanamo Bay detainees, *see* 2d Am. Compl. ¶ 3, have requested documents from defendants under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, relating to the highly classified Terrorist Surveillance Program ("TSP"), a program the President of the United States authorized after the terrorist attacks of September 11, 2001. Plaintiffs filed this lawsuit challenging defendants' response on two grounds. First, plaintiffs challenge the defendants' refusal to confirm or deny the existence of records concerning specific alleged targets of the TSP. *See* 2d Am. Compl. ¶ 8 (FOIA Request No. 1) (seeking to confirm or deny whether plaintiffs were targeted or subject to surveillance under the TSP). Second, plaintiffs challenge the withholding of certain records responsive to their request for "policies, procedures, guidelines, or practices for the interception of communications" under the TSP. *See id.* (FOIA Request No. 3). Only the former is at issue in this partial motion for summary judgment, with the latter issue to be resolved under a distinct briefing schedule. *See* Docket Entry 14 (Feb. 27, 2008).

At its core, this portion of plaintiffs' suit challenges the Government's "sweeping power" to protect intelligence sources and methods and classified information from public disclosure, *CIA v. Sims*, 471 U.S. 159, 169 (1985), and its broad authority to protect information concerning the NSA's operations. Plaintiffs seek an order compelling the defendants to confirm or deny the existence or non-existence of records "regarding, referencing, or concerning any of the plaintiffs" as related to the TSP, *i.e.*, TSP targeting information. *See* FOIA Request No. 1. The defendants properly refused to disclose this information because doing so would reveal: (i) information concerning the operations of the National Security Agency ("NSA") that is protected from disclosure by Section 6 of the National Security Agency Act, *see* 50 U.S.C. § 402 note;

(ii) intelligence sources and methods, which the Director of National Intelligence ("DNI") is charged with protecting from public disclosure under the National Security Act of 1947, as amended, 50 U.S.C. § 403-1; and (iii) information that is classified for reasons of national security under Executive Order ("E.O.") 12958, 60 Fed. Reg. 19825 (April 17, 1995), *as amended by* E.O. 13292, 68 Fed. Reg. 15315 (Mar. 25, 2003). The existence or non-existence of records pertaining to particular targets of the TSP has never been acknowledged because doing so would compromise the United States Intelligence Communities' sources and methods, including the manner in which the TSP operated, and the Nation's intelligence capabilities. Indeed, the only other court to consider an identical request for information that would confirm or deny whether a particular plaintiff was targeted by or subject to TSP surveillance had no trouble whatsoever concluding that a response refusing to confirm or deny was entirely lawful under FOIA. *See People for the American Way v. NSA*, 462 F. Supp. 2d 21, 27-32 (D.D.C. 2006).

The defendants therefore can neither confirm nor deny the existence of documents in response to plaintiffs' request without compromising the concerns that animate FOIA's exemptions from disclosure, and specifically the exemptions set forth at 5 U.S.C. §§ 552(b)(1) and (b)(3). Accordingly, the defendants properly refused to confirm or deny the existence of the documents responsive to plaintiffs' request, a response known as a "*Glomar* response." *See Phillippi v. CIA*, 546 F.2d 1009, 1011 (D.C. Cir. 1976). Settled law and policy rationales fully support these *Glomar* responses, which are well within the boundary of what the *Glomar* doctrine covers. And these determinations are fully supported by the public declarations submitted herewith because responding to this request would "would reveal information that is currently and properly classified in accordance with E.O. 12958 as amended and is protected from disclosure by statute." *See* Declaration of Joseph J. Brand ("Brand Decl.") ¶ 19, attached as

Exh. A. *See also* Declaration of J. Michael McConnell ("DNI Decl.") ¶ 16, attached as Exh. B. (concluding that revealing the kind of targeting information plaintiffs seek "would severely undermine surveillance activities in general, causing exceptionally grave harm to the national security of the United States.") Because these responses are lawful under FOIA, the defendants are entitled to partial summary judgment regarding the *Glomar* response.

FACTUAL BACKGROUND[1]

1. Origin and Mission of the NSA. The National Security Agency ("NSA" or "the Agency") was established by Presidential Directive in 1952 as a separately organized agency within the Department of Defense. Brand Decl. ¶ 4. NSA has three functions: to collect, process, and disseminate signals intelligence information for national foreign intelligence purposes; to conduct information security activities; and to conduct operations security training for the U.S. Government. *Id.*; *see also* Executive Order 12333, 46 Fed. Reg. 59941, § 1.12(b) (setting forth the responsibilities of the NSA).[2]

Signals intelligence ("SIGINT") is one of NSA's primary functions. Brand Decl. ¶ 5. NSA's SIGINT mission includes obtaining information from foreign electromagnetic signals and intercepting communications necessary to the national defense, national security, or the conduct of foreign affairs of the United States. *Id.* NSA provides, frequently on a rapid response basis,

---

[1] Defendants are not submitting a Statement pursuant to Local Civil Rule 56.1, in accordance with the general practice in this Circuit. *See Ferguson v. FBI*, No. 89 Civ. 5071, 1995 WL 329307, at *2 (S.D.N.Y. June 1, 1995), *aff'd*, 83 F.3d 41 (2d Cir. 1996). If the Court wishes Defendants to submit such a Statement, we will do so promptly.

[2] Executive Order 12333 has been twice amended, *see* 68 Fed. Reg. 4075 (Jan. 23, 2003); 69 Fed. Reg. 53593 (Aug. 27, 2004), to take account of the restructuring of the Intelligence Community that resulted from the creation of the Department of Homeland Security and the Office of the Director of National Intelligence.

reports derived from such information or data to national policy makers and the intelligence community of the United States Government. *Id.*

There are two primary reasons for gathering and analyzing intelligence information: the first, and most important, is to gain information required to direct U.S. resources as necessary to counter external threats. The second reason is to obtain information necessary to direct the foreign policy of the United States. *Id.* ¶ 7. Information produced by SIGINT is relevant to a wide range of issues, including military order of battle; threat warnings and readiness; arms proliferation; terrorism; and foreign aspects of international narcotics trafficking. *Id.*

The SIGINT collection mission of NSA provides national policy makers and the intelligence community with highly reliable foreign intelligence information. *Id.* ¶ 5. This information is often critical to the formulation of U.S. foreign policy and the support of U.S. military operations around the world. *Id.* ¶ 7. Foreign intelligence information produced by NSA as a result of its SIGINT mission is often unobtainable by other means. *Id.*

NSA's ability to produce foreign intelligence information depends upon its access to foreign and international electronic communications. *Id.* ¶ 9. Thus, NSA has developed a sophisticated worldwide SIGINT collection network to acquire these communications. *Id.* ¶ 8. The technological infrastructure that supports NSA's foreign intelligence information collection has taken years to develop at a substantial cost and untold human effort. *Id.* It relies on sophisticated collection and processing technology that is designed to keep pace with challenging new technological developments. *See id.* ¶¶ 8, 9

A fundamental tenet of NSA's communications collection process is that the identity of specific communications (referred to as "targets"), the degree of success in exploiting these targets, the vulnerability of particular foreign communications, and the extent of any cryptologic

successes are matters that must be maintained in the strictest secrecy. *Id.* ¶ 10. This is because NSA's SIGINT technology is both expensive and fragile. *Id.* ¶ 9. Disclosure of the identities of targets, the degree of success or weakness in exploiting those targets, the vulnerabilities of particular foreign communications, and the extent of any cryptologic success would encourage countermeasures by the targets of NSA's efforts. *Id.* ¶ 10. Public disclosure of either the capability to collect specific communications or the substance of the information itself can easily alert targets to the vulnerability of their communications. *Id.* ¶ 9. Thus, disclosure of even a single communication has the potential to reveal the intelligence collection techniques that are applied against targets around the world. *Id.*

Once alerted that NSA is targeting their communications, a target can easily frustrate SIGINT collection by taking steps to evade detection, to manipulate the information that NSA receives, or to implement other countermeasures aimed at undermining NSA's operations, such as, for example, using different communications techniques or utilizing a different communications link. *Id.* ¶ 10. If a target is successful in defeating an intercept operation, all of the intelligence from that source is lost until and unless NSA can establish a new and equivalent exploitation of the target's signals. *Id.* If a source becomes unavailable, the military, national policymakers, and the intelligence community must operate without the information such signals provided. *Id.* These intelligence losses are extremely harmful to the national security of the United States. *Id.* *See also* DNI Decl. ¶ 16.

2. **The Terrorist Surveillance Program**. Following the devastating attacks of September 11, 2001, the President of the United States authorized the NSA to intercept international communications into and out of the United States of persons linked to al Qaeda or related terrorist organizations (hereinafter, the "Terrorist Surveillance Program," or "TSP").

Brand Decl. ¶ 11. The TSP was a SIGINT program critical to the national security of the United States. *Id.* It was a targeted and focused program intended to help "connect the dots" between known and potential terrorists and their affiliates. *Id.* In order to intercept a communication under the TSP, one party to the communication must have been located outside the United States, and there must have been a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda. *Id.* Thus, the TSP was an "early warning system" established in order to detect and prevent another catastrophic attack on the United States.[3] *Id.*

The President publicly acknowledged the existence of the TSP on December 17, 2005. *Id.* ¶ 12. As the President has made clear, however, details about the TSP remain highly classified and subject to special access restrictions under the criteria set forth in Executive Order 12958, 60 Fed. Reg. 19825 (Apr. 17, 1995), as amended by Executive Order 13292, 68 Fed. Reg. 15315 (Mar. 25, 2003). *Id.* Unauthorized disclosure of information regarding the TSP can be expected to cause exceptionally grave damage to the national security of the United States, and thus, pursuant to the criteria outlined in Executive Order 12958, as amended, information related to the TSP is classified TOP SECRET. *Id.*; *see also* DNI Decl. ¶ 5. Moreover, because information related to the TSP involves or derives from particularly sensitive intelligence sources and methods, it is subject to the special access and handling procedures reserved for Sensitive

[3] On January 17, 2007, the Attorney General announced that any electronic surveillance that was occurring under the TSP would now be conducted subject to the approval of the Foreign Intelligence Surveillance Court and that the President's authorization of the TSP had lapsed. *See* DNI Decl. ¶ 13. Congress subsequently clarified and amended the Foreign Intelligence Surveillance Act through the Protect America Act, which itself lapsed on February 16, 2008. *Id.*

Compartmented Information ("SCI").[4] Brand Decl.¶ 12; *see also* DNI Decl. ¶ 5.

3. Plaintiffs' FOIA Request No. 1

On January 18, 2006, plaintiffs submitted a FOIA request to defendants seeking records regarding the TSP. *See* 2d Am. Compl. ¶ 8. Plaintiffs sought seven categories of records, but at issue in this motion is only plaintiffs' FOIA Request No. 1, which sought records "regarding, referencing, or concerning any of the plaintiffs" under the TSP. *Id.* *See also* Brand Decl. ¶¶ 15, 16 & attachments thereto; Declaration of David M. Hardy ("Hardy Decl.") ¶¶ 10-14 & attachments thereto, attached as Exh. C. Defendants refused to confirm or deny whether they had records responsive to this request. *See*, *e.g.*, Brand Decl. ¶ 16; Hardy Decl. ¶ 12.

ARGUMENT

DEFENDANTS PROPERLY REFUSED TO CONFIRM OR DENY THE EXISTENCE OF RECORDS RESPONSIVE TO PLAINTIFFS' REQUEST NUMBER 1 CONCERNING WHETHER THEY WERE SUBJECT TO TSP SURVEILLANCE

I. THE FREEDOM OF INFORMATION ACT AND EXEMPTIONS APPLICABLE TO DEFENDANTS' *GLOMAR* RESPONSE.

The FOIA's "basic purpose" reflects a "general philosophy of full agency disclosure unless information is exempted under clearly delineated statutory language." *John Doe Agency v. John Doe Corp.*, 493 U.S. 146, 152 (1989). "Congress recognized, however, that public disclosure is not always in the public interest." *Sims*, 471 U.S. at 166-67. The FOIA is thus designed to achieve a "workable balance between the right of the public to know and the need of the Government to keep information in confidence to the extent necessary without permitting

[4] Access to Sensitive Compartmented Information ("SCI") requires specialized clearance in addition to the 'Top Secret' level. "SCI is classified information that is required to be handled exclusively within formal access control systems established by the Director of [National] Intelligence." *Guillot v. Garrett*, 970 F.2d 1320, 1322 n. 1 (4th Cir. 1992).

indiscriminate secrecy." *John Doe*, 493 U.S. at 152 (quoting H.R. Rep. No. 1497, 89th Cong., 2 Sess. 6 (1966), *reprinted in* 1966 U.S.C.C.A.N. 2418, 2423). To that end, FOIA mandates disclosure of government records unless the requested information falls within one of nine enumerated exceptions, *see* 5 U.S.C. § 552(b). Despite the "liberal congressional purpose" of FOIA, the statutory exemptions must be given "meaningful reach and application." *John Doe*, 493 U.S. at 152. "Requiring an agency to disclose exempt information is not authorized . . . ." *Minier v. CIA*, 88 F.3d 796, 803 (9th Cir. 1996) (quoting *Spurlock v. Fed. Bureau of Investigation*, 69 F.3d 1010, 1016 (9th Cir. 1995)). Indeed, "[a] district court only has *jurisdiction* to compel an agency to disclose *improperly withheld* agency records," *i.e.*, records that do "not fall within an exemption." *Minier*, 88 F.3d at 803 (emphasis in original); *see also* 5 U.S.C. § 552(a)(4)(B) (providing jurisdiction only to "enjoin the agency from withholding agency records and to order the production of any agency records improperly withheld . . . .").

A. *Glomar* Responses Are Appropriate When An Agency Cannot Confirm Or Deny The Existence Of Records.

An agency's decision to neither confirm nor deny the existence of responsive records is commonly known as a "*Glomar*" response (in reference to the subject of a FOIA request for records pertaining to a ship, the "Hughes Glomar Explorer"). *See Phillippi v. CIA*, 546 F.2d 1009 (D.C. Cir. 1976). Invoking a *Glomar* response, as was done here with regard to FOIA Request No. 1, is appropriate when "to confirm or deny the existence of records . . . would cause harm cognizable under a FOIA exemption." *Gardels v. CIA*, 689 F.2d 1100, 1103 (D.C. Cir. 1982); *ACLU v. DOD*, 389 F. Supp. 2d 547, 558-66 (S.D.N.Y. 2005) (discussing the *Glomar* standard under Exemptions 1 and 3 and upholding in part and denying in part the CIA's *Glomar* response). *See also Earth Pledge Found. v. CIA*, 988 F. Supp. 623, 626 (S.D.N.Y. 1996)

(upholding a *Glomar* response refusing to confirm or deny the existence of a CIA field station), *aff'd* 128 F.3d 788 (2d Cir. 1997); *Daily Orange Corp. v. Central Intelligence Agency*, 532 F. Supp. 122, 124-26 (N.D.N.Y. 1982) (upholding a *Glomar* response refusing to confirm or deny covert activities at a university). The Government bears the burden of proving that the withheld information falls within the exemptions it invokes.[5] 5 U.S.C. § 552(a)(4)(b). The defendants invoked the *Glomar* response under Exemption 1 and Exemption 3; these exemptions are now discussed in turn.

B. Exemption 1 Protects From Disclosure Properly Classified Information Relating to the National Defense or Foreign Policy.

Exemption 1 protects records that are: (A) specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign policy, and (B) are in fact properly classified pursuant to an Executive Order.[6] *See* 5 U.S.C. §

---

[5] The Court should grant summary judgment if the movant shows, viewing the facts in the light most favorable to the nonmovant, that there are no genuine issues of material fact and that the movant is entitled to judgment as a matter of law. Fed. R. Civ. P. 56(c); *see Celotex Corp. v. Catrett*, 477 U.S. 317, 322-23 (1986). A party opposing summary judgment "may not rest upon the mere allegations or denials of his pleading, but . . . must set forth specific facts showing that there is a genuine issue for trial." *Anderson v. Liberty Lobby*, 477 U.S. 242, 248 (1986). In a FOIA case, the court may award summary judgment to an agency based on declarations that describe "the justifications for nondisclosure with reasonably specific detail, demonstrate that the information withheld logically falls within the claimed exemption, and are not controverted by either contrary evidence in the record nor by evidence of agency bad faith." *Military Audit Project v. Casey*, 656 F.2d 724, 738 (D.C. Cir. 1981).

[6] Section 1.2(a)(4) of Executive Order 12958, as amended, states that an agency may classify information that fits into one or more of the Executive Order's categories for classification when the appropriate classification authority "determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security." 68 Fed. Reg. 15315, 15315 (Mar. 25, 2003). Section 3.6(a) of E.O. 12958 further states that "an agency may refuse to confirm or deny the existence or nonexistence of requested records whenever the fact of their existence or nonexistence is itself classified under this order or its predecessors." *Id.* at 15324.

552(b)(1). Exemption 1 thus "establishes a specific exemption for defense and foreign policy secrets, and delegates to the President the power to establish the scope of that exemption by executive order." *Military Audit Project*, 656 F.2d at 737.

An agency can demonstrate that it has properly withheld information under Exemption 1 if it establishes that it has met the Executive Order's substantive and procedural requirements. In order to properly invoke Exemption 1, the agency must provide "detailed and specific" information demonstrating both "why the material has been kept secret and why such secrecy is allowed by the terms of an existing executive order." *ACLU v. United States Dep't of Justice*, 265 F. Supp. 2d 20, 27 (D.D.C. 2003). Substantively, this requires an agency to show that the records at issue logically fall within the exemption, *i.e.*, that the Executive Order authorizes the classification of the information. Procedurally, the proper procedures in classifying the information must be followed. *See Salisbury v. United States*, 690 F.2d 966, 970-73 (D.C. Cir. 1982); *Military Audit Project*, 656 F.2d at 737-38. An agency meeting both tests is then entitled to summary judgment. *See, e.g.*, *Abbotts v. NRC*, 766 F.2d 604, 606-08 (D.C. Cir. 1985); *Miller v. Casey*, 730 F.2d 773, 776 (D.C. Cir. 1984).

Agency decisions to withhold classified information under FOIA are reviewed de novo by the courts, and the agency bears the burden of proving its claim for exemption. *See* 5 U.S.C. § 552(a)(4)(B); *Miller*, 730 F.2d at 776. Nevertheless, in evaluating the applicability of FOIA exemptions for purposes of deciding this summary judgment motion, the Court must be mindful when the information sought by a plaintiff "implicat[es] national security, a uniquely executive purview." *Center for Nat'l Security Studies v. U.S. Dept. of Justice*, 331 F.3d 918, 926-27 (D.C. Cir. 2003). Numerous courts have specifically recognized the "propriety of deference to the executive in the context of FOIA claims which implicate national security." *Id.* at 927-29 (citing,

inter alia, Sims, supra; *McGehee v. Casey*, 718 F.2d 1137 (D.C. Cir. 1983)). *See also ACLU v. DOD*, 389 F. Supp. 2d 547, 562-63 (S.D.N.Y. 2005) (citing numerous cases). Thus, the courts must accord "substantial weight" to an agency's affidavits justifying classification when reviewing a claim under Exemption 1.[7] *Doherty v. DOJ*, 775 F.2d 49, 52 (2d Cir. 1985); *Military Audit Project*, 656 F.2d at 738 (noting that agencies' possess "unique insights" into the adverse effects that might result from public disclosure of classified information); *Earth Pledge Found.*, 988 F. Supp. at 626.

C. Exemption 3 Authorizes Withholding Under FOIA When A Separate Statute Protects Information And Here Three Such Statutes Are At Issue.

Exemption 3 applies when a separate statute protects information from disclosure. 5 U.S.C. § 552(b)(3). "A court evaluating an agency's refusal to comply with a FOIA request under section 552(b)(3) must ask two questions: First, is the statute in question a statute of exemption as contemplated by section 552(b)(3), and second, does the withheld information satisfy the criteria of the exemption statute." *See Earth Pledge Found.*, 988 F. Supp. at 627 (citing *Fitzgibbon v. CIA*, 911 F.2d 755, 761 (D.C. Cir. 1990)). Because the threshold issue for the application of Exemption 3 is based on the statute invoked by the agency, the analysis is distinct from that employed to analyze other FOIA exemptions. As the D.C. Circuit has

---

[7] Indeed, courts have routinely and repeatedly emphasized that "weigh[ing] the variety of subtle and complex factors in determining whether disclosure of information may lead to an unacceptable risk of compromising the [nation's] intelligence-gathering process" is a task best left to the Executive Branch and not attempted by the judiciary. *Sims*, 471 U.S. at 180; *see also Center for Nat'l Security Studies*, 331 F.3d at 928 ("the judiciary is in an extremely poor position to second-guess the executive's judgment in [the] area of national security"); *Halperin v. CIA*, 629 F.2d 144, 148 (D.C. Cir. 1980) ("Judges . . . lack the expertise necessary to second-guess [] agency opinions in the typical national security FOIA case"). Thus, although review of an agency's response to FOIA is *de novo*, courts have thus "consistently deferred to executive affidavits predicting harm to national security, and have found it unwise to undertake searching judicial review." *Center for Nat'l Security Studies*, 331 F.3d at 927.

explained, "'Exemption 3 differs from other FOIA exemptions in that its applicability depends less on the detailed factual contents of specific documents; the sole issue for decision is the existence of a relevant statute and the inclusion of withheld material within the statute's coverage.'" *Fitzgibbon*, 911 F.2d at 761-62 (quoting *Assoc. of Retired R.R. Workers v. United States R.R. Retirement Bd.*, 830 F.2d 331, 336 (D.C. Cir. 1987)). Here, several protective statutes encompass the information sought by plaintiffs regarding whether they were targets of or subject to TSP surveillance, and these statutes therefore authorize the Government to refuse to confirm the existence or non-existence of records under FOIA Exemption 3.

Foremost among them is Section 6 of the National Security Agency Act of 1959, Pub. L. No. 86-36, § 6, 73 Stat. 63, 64, codified at 50 U.S.C. § 402 note, which provides:

> [N]othing in this Act or any other law . . . shall be construed to require the disclosure of the organization or any function of the National Security Agency, of any information with respect to the activities thereof, or of the names, titles, salaries, or number of persons employed by such agency.

It is well-established that Section 6 "is a statute qualifying under Exemption 3." *The Founding Church of Scientology of Washington, D.C., Inc. v. Nat'l Security Agency*, 610 F.2d 824, 828 (D.C. Cir. 1979). Section 6 reflects a "congressional judgment that in order to preserve national security, information elucidating the subjects specified ought to be safe from forced exposure." *Church of Scientology*, 610 F.2d at 828. In enacting Section 6, Congress was "fully aware of the 'unique and sensitive' activities of the [NSA] which require 'extreme security measures.'" *Hayden v. NSA/CSS*, 608 F.2d 1381, 1390 (D.C. Cir. 1979) (citing legislative history). Thus, as the D.C. Circuit has held, "[t]he protection afforded by section 6 is, by its very terms, absolute. If a document is covered by section 6, NSA is entitled to withhold it . . . ." *Linder v. NSA*, 94 F.3d 693, 698 (D.C. Cir. 1996).

The second applicable statute is Section 102A(i)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (Dec. 17, 2004), codified at 50 U.S.C. § 403-1(i)(1). This statute requires the Director of National Intelligence to "protect intelligence sources and methods from unauthorized disclosure." It is "settled" that this statute falls within Exemption 3. *Gardels*, 689 F.2d at 1103 (discussing predecessor statute applicable to CIA, which provided that "the Director of Central Intelligence shall be responsible for protecting intelligence sources and methods from unauthorized disclosure"); *accord Sims*, 471 U.S. at 167-68, 193; *Earth Pledge Found.*, 988 F. Supp. at 627 (holding that the predecessor statute to the current statute giving the DNI the authority to protect sources and methods is "clearly [an] exemption statute[] for the purpose of section 552(b)(3)").[8] *See also Hogan v. Huff*, 2002 WL 1359722, * 8 (S.D.N.Y. 2002).

The third applicable statute is 18 U.S.C. § 798. This statute prohibits, on pain of criminal penalty, the disclosure of various kinds of classified information, including information "concerning the communications intelligence activities of the United States." 18 U.S.C. § 798 Specifically, 18 U.S.C. § 798(a) provides, in pertinent part, that:

> Whoever knowingly and willfully communicates, furnishes, transmits or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States . . . any classified information . . . (3) concerning the communications intelligence activities of the United States . . . shall be fined under this title or imprisoned for not more than ten years, or both.

The term "communications intelligence" means "all procedures and methods used in the

---

[8] The predecessor statute was superceded by enactment of the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (Dec. 17, 2004), which shifted the responsibility for protecting intelligence sources and methods from the Director of Central Intelligence to the Director of National Intelligence.

interception of communications and the obtaining of information from such communications by other than the intended recipients." *Id.* § 798(b). This statute clearly identifies matters to be withheld from the public and refers to particular types of matters to be withheld. *See* 5 U.S.C. § 552(b)(3). Thus, this statute qualifies as an Exemption 3 statute under FOIA. *See Florida Immigrant Advocacy Ctr. v. Nat'l Security Agency*, 380 F. Supp. 2d 1332, 1340 (S.D. Fla. 2005) ("Other exempting statutes include . . . 18 U.S.C. § 798"); *Winter v. Nat'l Security Agency*, 569 F. Supp. 545 (S.D. Cal. 1983) (18 U.S.C. § 798 is a "statute[] within Exemption 3").

Because these statutes unquestionably meet the first prong of the exemption 3 inquiry, the sole question is whether the information sought "satisf[ies] the criteria of the exemption statute." *Earth Pledge Found.*, 988 F. Supp. at 627.

II. UNDER THE APPLICABLE EXEMPTIONS, THE DEFENDANTS PROPERLY REFUSED TO CONFIRM OR DENY THE EXISTENCE OF INFORMATION REGARDING WHETHER PLAINTIFFS WERE TARGETS OF THE TSP.

FOIA Request No. 1 seeks, as related to the TSP, "a list of records . . . regarding, referencing, or concerning any of the plaintiffs." *See* 2d Am. Compl. ¶ 8. At bottom, this request seeks information relating to the identity of particular alleged targets of and/or who may have been subject to surveillance under the TSP. Brand Decl. ¶¶ 15, 18. The *Glomar* response—refusing to confirm or deny the existence of records concerning particular alleged targets of surveillance under the TSP—is entirely proper.

Courts routinely affirm the right of the Government to assert a *Glomar* response for information concerning surveillance of particular individuals. In *Marrera v. U.S. Dept. of Justice*, 622 F. Supp. 51 (D.D.C. 1985), for example, a federal prisoner sought records from, among other entities, the Office of Intelligence Policy and Review seeking to confirm or deny that he had been subject to surveillance under FISA. Citing Exemption 1, the Court upheld the

Government's decision refusing to confirm or deny whether particular individuals were the target of surveillance under a Foreign Intelligence Surveillance Court warrant. *Id.* at 53 (discussing how the mere acknowledgment of "the *existence* of such records would implicitly *reveal* classifiable information") (emphasis in original). *See also Arabian Shield Development Co. v. CIA*, 1999 WL 118796, *2-3 (N.D. Tex. 1999) (holding that CIA properly refused to confirm or deny whether it "has collected intelligence regarding specific individuals or corporations, or has an intelligence interest or a facility in a particular foreign location"). This common sense conclusion, without a doubt, stems from the paramount need for secrecy of surveillance in order to obtain useful intelligence information. *See, e.g.*, *Fitzgibbon*, 911 F.2d at 763; *see* DNI Decl. ¶ 16 (concluding in light of the unworkability of disclosing such information that "[t]he only viable way for the Intelligence Community to protect this intelligence collection mechanism, accordingly, is neither to confirm nor deny whether someone has been targeted or subject to surveillance collection, regardless of whether the individual has been targeted.").

If the Intelligence Community were required to affirmatively or negatively respond to each of requests from particular individuals seeking to confirm or deny whether they were targeted by or subject to TSP surveillance, critically important surveillance strategies would hardly remain confidential. *See, e.g.*, *Bassiouni v. Central Intelligence Agency*, 392 F.3d 244, 246 (7th Cir. 2004). Indeed, as courts have recognized, any information available to a FOIA requester is similarly available to "North Korea's secret police and Iran's counterintelligence service too." *Id.* These and "other hostile entities," *id.*, including agents of al Qaeda and its affiliates, would no doubt be greatly interested in the opportunity to have the Government officially and publicly confirm or deny whether they or others are subjects of surveillance under the TSP. For this reason, as the Seventh Circuit has therefore noted, "[e]very appellate court to

address the issue has held that the FOIA permits the [intelligence agencies] to make a 'Glomar response' when it fears that inferences from . . . selective disclosure could reveal classified sources or methods of obtaining foreign intelligence." *Id.* ("when a pattern of responses itself reveals classified information, the *only way to keep secrets is to maintain silence uniformly*") (emphasis added).

Quite consistent with this approach, the only other court to consider the Government's *Glomar* response to a plaintiff's request for TSP targeting information upheld the NSA's refusal to confirm or deny the existence of records concerning whether they had been the target of or subject to surveillance under the TSP. Like plaintiffs here, in *People for the American Way v. NSA*, 462 F. Supp. 2d 21 (D.D.C. 2006) ("*PFAW*"), the plaintiff made FOIA requests concerning the TSP and sought, *inter alia*, any "records related to the surveillance of plaintiff." *Id.* at 29. Affording due deference to the NSA's explanations, the Court concluded that the *Glomar* response was proper under both Exemption 3, *id.* at 29-30, and Exemption 1. *Id.* at 32. Here, as in *PFAW*, Exemption 1 and Exemption 3 fully and independently support the refusal to confirm or deny the existence of records responsive to requests that seek information regarding whether particular persons are the target of surveillance under the TSP.

A. Defendants' Glomar Response is Justified Under Exemption 1.

In light of the exceptionally grave danger to national security that would reasonably be expected to result from confirming or denying whether records exist as to whether particular individuals were targeted by or subject to surveillance under the TSP, this information is currently and properly classified under the terms of Executive Order 12958, as amended. Thus, because the fact of the existence or nonexistence of the information requested in plaintiffs' FOIA Request No. 1 is a currently and properly classified matter in accordance with Executive Order

12958, as amended, it therefore was properly withheld under Exemption 1. *See PFAW*, 462 F. Supp. 2d at 32 (holding that TSP targeting information is properly subject to a *Glomar* response under Exemption 1). *See also Marrera*, 622 F .Supp. at 53 (upholding, under Exemption 1, *Glomar* response to request of information concerning whether particular individuals were the target of surveillance under a FISC warrant). The defendants are therefore entitled to partial summary judgment.

Substantively and procedurally, it is unquestionably clear that information confirming or denying whether particular individuals were targeted or otherwise subject to surveillance under the TSP is properly classified and that the release of that information would harm the national security. As explained, as a general matter information concerning the TSP's operation is classified TOP SECRET, *see* Brand Decl., ¶ 12; DNI Decl. ¶ 5; Hardy Decl. ¶ 7, and revealing the "existence or non-existence of surveillance information that reference the Plaintiffs was proper because a positive or negative response to this request would reveal information that is currently and properly classified." Brand Decl. ¶ 19. In particular, it has been determined that any "[a]cknowledgment of the existence or non-existence of surveillance information referencing the Plaintiffs would reveal information that meets the criteria for classification as set forth in Subparagraphs (c) and (g) of Section 1.4 of Executive Order 12958 . . . which authorizes the classification of information concerning 'intelligence activities . . . intelligence sources and methods, or cryptology' and 'vulnerabilities or capabilities of systems . . . relating to national security." *Id.* ¶ 20. *See also* DNI Decl. ¶¶ 5, 19. Revealing the existence of records that would confirm or deny whether particular individuals were targeted by or subject to surveillance under the TSP, as is the case with plaintiffs' FOIA Request No. 1, obviously implicates these portions of the Executive Order.

Because of the highly classified nature of the TSP, NSA cannot confirm publicly in any particular case whether any communications were collected pursuant to the TSP or, conversely, that such communications were not collected:

> Confirmation by NSA that a person's activities are not of foreign intelligence interest or that NSA is unsuccessful in collecting foreign intelligence information on their activities on a case-by-case basis would allow our adversaries to accumulate information and draw conclusions about NSA's technical capabilities, sources, and methods. For example, if NSA were to admit publicly in response to an information request that no information about Persons X, Y or Z exists, but in response to a separate information request about Person T state only that no response could be made, this would give rise to the inference that Person T is a target of the TSP. Over time, the accumulation of these inferences would disclose the targets and capabilities (sources and methods) of the TSP and inform our adversaries of the degree to which NSA is aware of some of their operatives or can successfully exploit particular communications.

Brand Decl. ¶ 22; *Bassiouni*, 392 F.3d at 246. *See also* DNI Decl. ¶ 16 ("providing assurances that someone is not being targeted becomes unworkable, and itself revealing, in cases where an individual may be targeted . . . [because] a refusal to confirm or deny only in cases where surveillance is occurring would effectively disclose . . . surveillance.); Hardy Decl. ¶¶ 17-18. The Director of National Intelligence explains that either confirming or denying the existence of surveillance targeting information would reveal critical information:

> To confirm or deny whether someone is a target of surveillance would disclose either who is being targeted—thus compromising that collection—or who is not being targeted. This would reveal to our adversaries that an individual may or may not be available as a secure means for communicating or, more broadly, the methods being used to conduct surveillance. Confirmation of a target's identity would immediately disrupt the flow of accurate intelligence as the target takes steps to evade detection or manipulate the information received. And while it may seem innocuous to disclose that law-abiding citizens are not being targeted, this may provide insight to a trained eye as to the scope or the NSA's activities.

DNI Decl. ¶ 16. The Intelligence Community cannot respond to each case in isolation, but must assume that the United States's adversaries will examine all released information together.

Brand ¶ 23. *See also* DNI Decl. ¶ 17; Hardy Decl. ¶ 20. The disclosure of information from which our adversaries can ascertain the capabilities of the NSA, the frequency with which it intercepts communications, or the types of targets it intercepts poses the danger that targets will adapt their behavior in an effort to evade detection. *See, e.g.*, Brand Decl. ¶¶ 21-22; Hardy Decl. ¶ 18.

Providing this kind of information in a public forum would be "invaluable" to this Nation's enemies. *See* Brand Decl. ¶ 21; Hardy Decl. ¶ 17 (providing such information would give "a road map" to the Nation's adversaries). Because our ability to produce foreign intelligence information depends upon its access to foreign and international electronic communications, public disclosure of either the capability to collect specific communications, the substance of the information derived from such collection, or the frequency with which such information is collected "can easily alert targets to the vulnerability of their communications." *See* Brand Decl. ¶ 9. Once alerted, SIGINT targets can "implement measures to thwart continued SIGINT collection." *Id.* Thus, "[i]f an individual learns or suspects that his signals are or may be targeted by the NSA for collection, he can take steps to evade detection, to manipulate the information that NSA receives, or to implement other countermeasures aimed at undermining NSA's operations." *Id.* ¶ 13. Such efforts to evade NSA monitoring would deny the United States access to information crucial to the defense of the United States. *See* Brand Decl. ¶ 10; *see Center for Nat'l Security Studies*, 331 F.3d at 933.

For this reason, it has been determined that to confirm or deny the existence of targeting information as to particular individuals "would result in the frequent, routine exposure of intelligence information, sources, and methods and would severely undermine surveillance activities in general, causing exceptionally grave harm to the national security of the United

States." DNI Decl. ¶ 16. *See also* Brand Decl. ¶¶ 21-23; Hardy Decl. ¶ 19. *Gardels*, 689 F.2d at 1104 (describing the dangers of accumulated information that might be provided in response to FOIA requests); *Gordon v. Fed. Bureau of Investigation*, 388 F. Supp. 2d 1028, 1037 (N.D. Cal. 2005) (same).

B. Exemption 3 Independently Supports Defendants' Glomar Response

The fact of the existence or nonexistence of records is also protected from disclosure by federal statute and, thus, properly withheld under Exemption 3.

Acknowledging the existence or nonexistence of the information requested by Plaintiffs' FOIA Request No. 1 would unquestionably reveal NSA's organization, functions and activities by revealing the success or failure of NSA's activities. Brand Decl. ¶¶ 25, 30. Section 6 of the National Security Agency Act of 1959 clearly protects this information from disclosure. Information that relates to SIGINT collection—such as whether particular persons were subject to surveillance under the TSP (a SIGINT activity)—is exempt from disclosure, and thus need not be confirmed or denied, under Exemption 3. *See PFAW*, 462 F. Supp. 2d at 29-30. *See also Linder*, 94 F.3d at 696 ("There can be no doubt that the disclosure of [information related to SIGINT collection] would reveal information concerning the activities of the agency"); *Hayden*, 608 F.2d at 1389 ("signals intelligence is one of the NSA's primary functions"; and the release of information related to SIGINT collection would "disclose information with respect to [NSA] activities, since an intercepted communication concerns an NSA activity").

Confirming the existence or non-existence of records related to targets of surveillance would also reveal the sources and methods by which NSA collects foreign intelligence information. Brand Decl. ¶ 30; *see also* DNI Decl. ¶¶ 15-16, 18 (invoking his statutory authority to protect sources and methods). Section 102A(i)(1) of the Intelligence Reform and Terrorism

Prevention Act of 2004 specifically authorizes the withholding of this kind of information. The authority to protect intelligence sources and methods from disclosure is rooted in the "practical necessities of modern intelligence gathering," *Fitzgibbon*, 911 F.2d at 760, and has been described by the Supreme Court as both "sweeping," *Sims*, 471 U.S. at 169, and "wideranging." *Snepp v. United States*, 444 U.S. 507, 509 (1980). Sources and methods constitute "the heart of all intelligence operations," *Sims*, 471 U.S. at 167, and "[i]t is the responsibility of the [intelligence community], not that of the judiciary to weigh the variety of complex and subtle factors in determining whether disclosure of information may lead to an unacceptable risk of compromising the . . . intelligence-gathering process." *Id.* at 180. As the declarations make clear, confirming or denying the existence of record here concerns "intelligence sources and methods" and thus falls squarely within the scope of Section 102A(i)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (Dec. 17, 2004), codified at 50 U.S.C. § 403-1(i)(1). *See* DNI Decl. ¶¶ 16, 18; *Fitzgibbon*, 911 F.2d at 762 (affirming agency decision to withhold information "relat[ing] to intelligence sources and methods"); *Linder*, 94 F.3d at 696 (upholding withholding of SIGINT collection information because "it seems obvious" that "disclosure could reveal information about NSA's capabilities and techniques that could be used by foreign governments to the detriment of U.S. national security interests"); *see also Sims*, 472 U.S. at 175 ("forced disclosure of the identities of its intelligence sources could well have a devastating impact on the [CIA]'s ability to carry out its mission"). *See also* Brand Decl. ¶¶ 30; Hardy Decl. ¶ 21.

Finally, confirming the existence or non-existence of this information would reveal the extent or limitations of NSA SIGINT capabilities. Brand Decl. ¶ 30. Revealing communications intelligence capabilities and limitations is clearly prohibited by 18 U.S.C. § 798. *See* pp. 13-14,

supra.

Because statutes of exemption clearly cover the information plaintiffs seek regarding whether or not they were targets of or otherwise subject to TSP surveillance, defendants properly relied on FOIA Exemption 3 in refusing to confirm or deny the existence of the information plaintiff requested.. *See PFAW*, 462 F. Supp. 2d at 29-30 (holding that TSP targeting information is subject to *Glomar* response under Exemption 3); *Gardels*, 689 F.2d at 1104 (upholding, under Exemption 3, an intelligence agency's refusal to confirm or deny the identity of persons with whom it had covert contacts). It is well-established that when relying on Exemption 3 as the basis for withholding, defendants are "not required to provide any information as to the particular security threats posed by the release of the documents. . . . '[a] specific showing of potential harm to national security . . . is irrelevant to the language of [section 6]. Congress has already decided that disclosure of NSA activities is potentially harmful.'" *Linder*, 94 F.3d at 696 (quoting *Hayden*, 608 F.2d at 1390). The same is true for the DNI's authority to protect intelligence sources and methods. Nonetheless, the accompanying declarations plainly demonstrate the serious consequences to the national security of the United States that would result from the disclosure of the information plaintiff seeks. *See* Brand Decl. ¶¶ 20-21; DNI Decl. ¶¶ 15-19; Hardy Decl. ¶¶ 17-20. *See also* pp. 16-18, *supra* (discussing the exceptionally grave harm to national security that would result from the disclosure of information related to the TSP which has been designated TOP SECRET-SCI under the terms of Executive Order 12958, as amended).

Congress' determination that information such as that at issue in this case should not be made public, *see* 50 U.S.C. § 402 note and 50 U.S.C. § 403-1(i), is strongly supported by the specific dangers NSA has identified that would result from such a disclosure. As to plaintiffs'

FOIA Request No. 1, accordingly, summary judgment should be granted to defendants.

CONCLUSION

For the foregoing reasons, the Defendants are entitled to summary judgment as to their Glomar response to plaintiffs' FOIA Request No. 1.

Dated: March 18, 2008

Respectfully Submitted,

JEFFREY S. BUCHOLTZ
Acting Assistant Attorney General

JOSEPH H. HUNT
Director, Federal Programs Branch

ELIZABETH A. SHAPIRO
Assistant Director, Federal Programs Branch

/s/ Alexander K. Haas
ALEXANDER K. HAAS (CA# 220932)
Trial Attorney
Federal Programs Branch, Civil Division
United States Department of Justice
P.O. Box 883, 20 Massachusetts Ave., N.W.
Washington, D.C. 20044
Tel: (202) 305-9334 — Fax: (202) 305-3138
Email: alexander.haas@usdoj.gov