[ORAL ARGUMENT SCHEDULED FOR MARCH 20, 2012]

No. 11-5233

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

ELECTRONIC PRIVACY INFORMATION CENTER,

Plaintiff-Appellant,

v.

NATIONAL SECURITY AGENCY,

Defendant-Appellee.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

BRIEF FOR APPELLEE

TONY WEST
Assistant Attorney General

RONALD C. MACHEN, JR.
United States Attorney

DOUGLAS N. LETTER
(202) 514-3602
CATHERINE Y. HANCOCK
(202) 514-3469
Attorneys, Appellate Staff
Civil Division, Room 7236
Department of Justice
Washington, D.C. 20530-0001

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

Pursuant to Circuit Rule 28(a)(1), appellees hereby certify as follows:

A. Parties and Amici.

The parties before this Court and the district court are: plaintiff-appellant the Electronic Privacy Information Center, a non-profit corporation, and defendant-appellee the National Security Agency. There are no intervenors or amici.

B. Ruling Under Review.

Plaintiff-appellant appeals from the district court's opinion and order (Richard J. Leon, J.) of July 8, 2011 (entered on July 13, 2011), granting summary judgment in favor of the National Security Agency and denying summary judgment for the Electronic Privacy Information Center. The district court's opinion and order of dismissal is published at 798 F.Supp.2d 26 (D.D.C. 2011).

C. Related Cases.

This case has not previously been before this Court and counsel is not aware of any related cases within the meaning of Circuit Rule 28(a)(1)(C).

Respectfully submitted,

s/Catherine Y. Hancock
CATHERINE Y. HANCOCK
Counsel for Defendant-Appellee

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

Cases:

---

* Authorities chiefly relied upon are marked with an asterisk.

Statutes:

Rules:

Miscellaneous:

GLOSSARY

Br.. . . . . Appellant's Opening Brief

EPIC.. . . . . Electronic Privacy Information Center

FOIA. . . . . Freedom of Information Act

JA.. . . . . Joint Appendix

NSA. . . . . National Security Agency

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

No. 11-5233

ELECTRONIC PRIVACY INFORMATION CENTER,

Plaintiff-Appellant,

v.

NATIONAL SECURITY AGENCY,

Defendant-Appellee.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

BRIEF FOR APPELLEE

STATEMENT OF JURISDICTION

In this action under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, plaintiff invoked the jurisdiction of the district court pursuant to 5 U.S.C. § 552(a)(4)(B) and 28 U.S.C. § 1331. Joint Appendix ("JA") 1. The district court entered final judgment for defendant-appellee, the National Security Agency, on July 13, 2011. JA 116. Plaintiff filed a timely notice of appeal on September 9, 2011. JA 117; Fed. R. App. P. 4(a)(1)(B). This Court has jurisdiction under 28 U.S.C. § 1291.

STATEMENT OF THE ISSUE

Whether NSA's "*Glomar* response," refusing to confirm or deny the existence of any records responsive to plaintiff's FOIA request, was proper because stating whether any such records exist, or do not exist, would reveal information protected from disclosure by FOIA Exemption 3, 5 U.S.C. § 552(b)(3).

STATUTES AND REGULATIONS

The pertinent statutory provisions, 5 U.S.C. § 552(b)(3), and Section 6 of the National Security Agency Act of 1959, Pub. L. No. 86-36, 73 Stat. 63, 64 (codified at 50 U.S.C. § 402 note), are reproduced in a statutory addendum at the conclusion of this brief.

STATEMENT OF THE CASE

Plaintiff-appellant, the Electronic Privacy Information Center ("EPIC"), requested records from the National Security Agency ("NSA") under the FOIA, concerning an alleged cooperative research and development agreement reached in early 2010 between defendant NSA and Google, Inc. ("Google"), as well as other alleged communications between NSA and Google regarding certain Google technologies. JA 14-17. NSA issued a "*Glomar* response" pursuant to FOIA Exemption 3, indicating that it could neither confirm nor deny whether any

responsive records exist.[1] JA 20-21. Plaintiff filed a complaint in district court challenging NSA's *Glomar* response. JA 1-7. The parties cross-moved for summary judgment, and the district court entered judgment for defendant. JA 116. Plaintiff appeals.

STATEMENT OF THE FACTS

A. Statutory Background

The Freedom of Information Act, 5 U.S.C. § 552, generally provides access to certain agency records and other information unless exempted by the statute. Section 552(a) provides that "[e]ach agency shall make available to the public" records in its possession unless the information is specifically exempted by one of Section 552(b)'s nine statutory exemptions.

FOIA Exemption 3, 5 U.S.C. § 552(b)(3), shields from disclosure records that are "specifically exempted from disclosure by statute * * * provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld." 5 U.S.C. § 552(b)(3).

---

[1] An agency's decision to neither confirm nor deny the existence of responsive records is referred to as a "'*Glomar* response,' taking its name from the *Hughes Glomar Explorer*, a ship built (we now know) to recover a sunken Soviet submarine, but disguised as a private vessel for mining manganese nodules from the ocean floor." *Bassiouni* v. *CIA*, 392 F.3d 244, 246 (7th Cir. 2004).

As this Court has already held, one such statute exempting disclosure is Section 6 of the National Security Agency Act of 1959, Pub. L. No. 86-36, 73 Stat. 63, 64 (codified at 50 U.S.C. § 402 note). *See Hayden* v. *NSA*, 608 F.2d 1381, 1389 (D.C. Cir. 1979); *Founding Church of Scientology* v. *NSA*, 610 F.2d 824, 828 (D.C. Cir. 1979) (holding that Section 6 "satisfies the strictures of Subsection (B)" of FOIA Exemption 3). That statute provides that "[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, [or] of any information with respect to the activities thereof [.]" § 6, 73 Stat. at 64. Accordingly, if agency records are protected from disclosure by Section 6, those records may properly be withheld pursuant to FOIA Exemption 3. *Larson* v. *Department of State*, 565 F.3d 857, 868 (D.C. Cir. 2009) (agency "need only demonstrate that the withheld information relates to the organization of the NSA or any function or activities of the agency" to withhold information pursuant to Exemption 3).

In addition to withholding records that are exempt, an agency may also refuse to confirm or deny the existence or nonexistence of records responsive to a FOIA request if the particular FOIA exemption at issue "would itself preclude the acknowledgment of such documents." *Minier* v. *CIA*, 88 F.3d 796, 800 (9th Cir. 1996); *accord Moore* v. *CIA*, ___ F.3d ___, 2011 WL 6355313, *2 (D.C. Cir. Dec.

20, 2011); *Wolf* v. *CIA*, 473 F.3d 370, 374 (D.C. Cir. 2007). Such a response is referred to as a *Glomar* response.

B. Plaintiff's FOIA Request and Proceedings Below

On February 4, 2010, plaintiff EPIC submitted a FOIA request to NSA. JA 14-17. EPIC's FOIA request noted recent media reports that Google and NSA had entered into a "partnership" or "cooperative research and development agreement" in the wake of a January 12, 2010 cyber attack on "Google's corporate infrastructure" by hackers in China. JA 14-15. In light of those reports, EPIC requested three categories of records from the NSA:

> 1. All records concerning an agreement or similar basis for collaboration, final or draft, between the NSA and Google regarding cyber security;
>
> 2. All records of communication between NSA and Google concerning Gmail, including but not limited to Google's decision to fail to routinely encrypt Gmail messages prior to January 13, 2010; and
>
> 3. All records of communications regarding NSA's role in Google's decision regarding the failure to routinely deploy encryption for cloud-based computing service, such as Google Docs.

JA 16.

NSA responded to EPIC's request on March 10, 2010. JA 20-21. NSA explained that, "[a]s part of its longstanding Information Assurance mission, NSA works with a broad range of commercial partners and research associates to ensure

the availability of secure tailored solutions for the Department of Defense and national security systems customers today and cutting-edge technologies that will secure the information systems of tomorrow." JA 20. Noting, however, that it is "authorized by statute to protect information concerning its functions and activities," NSA stated that it could "neither confirm nor deny whether [Google] has a relationship with the Agency related to the issues [EPIC] describe[d]" in its request. JA 20. NSA invoked FOIA Exemption 3, and Section 6 of the National Security Agency Act, as justification for its *Glomar* response. JA 20-21.

EPIC filed an administrative appeal, arguing that NSA's response was unlawful. JA 23-25. Prior to the resolution of that administrative appeal, however, EPIC filed suit in the United States District Court for the District of Columbia, challenging NSA's *Glomar* response. JA 1-7; *see also* JA 107-08. The parties cross-moved for summary judgment.

In support of its motion for summary judgment, NSA filed a declaration by Diane M. Janosek, NSA Deputy Associate Director for Policy and Records. JA 47-54. That declaration explained that one of NSA's primary cryptologic missions is its "Information Assurance mission," under which NSA is tasked with "protecting Department of Defense and other national-security information systems," and providing support to other agencies that protect "the nation's critical infrastructure

and key resources." JA 48. The declaration noted that NSA focuses primarily on discovering vulnerabilities in those information systems, monitoring malicious activity, security testing, and "provid[ing] or oversee[ing] cryptography for national-security systems" in its effort to ward off "ever-growing threats to [U.S. government] information systems." JA 49.

Because the "U.S. government is largely dependent on commercial technology for its information systems," including word processing programs and e-mail software, and "has worked with commercial vendors to develop and produce cryptographic products for use by the U.S. government," NSA routinely monitors security vulnerabilities in those commercial technologies and cryptographic products. JA 49. NSA further explained that such monitoring "is dependent on information from a number of intelligence and open sources in order to have early awareness of potential malicious activity or vulnerabilities." JA 49. If NSA determines that certain security vulnerabilities or malicious attacks pose a threat to U.S. government information systems, NSA may take action. JA 50.

For those reasons, the Janosek Declaration explained that confirming or denying the existence of the records EPIC sought would reveal whether NSA determined that "vulnerabilities or cybersecurity issues pertaining to Google or certain of its commercial technologies could make U.S. government information

systems susceptible to exploitation or attack by adversaries and, if so, whether NSA collaborated with Google to mitigate them." JA 52-53. NSA further explained that acknowledging whether or not NSA and Google did form a partnership resulting from a specific malicious attack "would reveal whether or not NSA considered the alleged attack to be of consequence for critical U.S. government information systems." JA 53. Such information would reveal NSA's functions and activities with respect to its Information Assurance mission, and could also "alert our adversaries to NSA priorities, threat assessments, or countermeasures that may or may not be employed against future attacks." JA 53.

C. District Court Decision

The district court held that NSA was entitled to summary judgment. The court explained that, "[i]t is well established that Section 6 of the NSA Act is a statutory exemption under Exemption 3," and that Section 6 "broadly prohibits the disclosure of information pertaining to the organization, function, or activities of the NSA." JA 111.

The court then turned to the NSA's affidavit in support of its *Glomar* response, and concluded that the Janosek Declaration "contains sufficient detail, pursuant to Section 6, to support NSA's claim that the protected information [sought by EPIC] pertains to" NSA's organization, functions, or activities. JA 112. As the court

explained, plaintiff's FOIA request "relates to the NSA's cryptologic Information Assurance mission," which "includes the assessment of commercial technologies and the Agency's participation in public-private security initiatives." JA 113. Specifically, "with respect to plaintiff's first request – all records concerning an agreement between NSA and Google regarding cyber-security – the Janosek Declaration explains that 'any acknowledgment by NSA of the existence or nonexistence of a relationship or agreement with Google * * * would reveal whether or not NSA considered the alleged attack to be of consequence for critical U.S. government information systems.'" JA 113. And, "with respect to plaintiff's second and third requests – NSA/Google communications regarding encryption of Gmail and cloud-based computing service, such as Google Docs – the Janosek Declaration clarifies that 'to confirm or deny the existence of any such records would be to reveal whether NSA, in fulfilling one of its key missions, determined that vulnerability or cyber security issues pertaining to Google or certain of its commercial technologies could make U.S. government information systems susceptible to exploitation or attack by adversaries * * * .'" JA 113.

The district court rejected plaintiff's argument that NSA's declaration was conclusory, stating that the declaration "explains the relevance of the Information Assurance mission to national security, the clear tie between the requested

information and the Information Assurance mission, and the cognizable harm posed by acknowledging the existence/non-existence of the information." JA 114. The district court also rejected plaintiff's argument that public dissemination of information about a potential Google-NSA relationship waived the agency's FOIA protection. JA 112. In sum, because the district court found NSA's declaration to be "both logical and plausible," the court upheld NSA's *Glomar* response. JA 114.

SUMMARY OF ARGUMENT

In this FOIA case, plaintiffs seek disclosure of NSA records that relate to an alleged partnership between Google and NSA, arising out of a cyber attack on Google by hackers in China, and communications between Google and NSA concerning certain Google technologies. NSA asserted a "*Glomar* response," refusing to confirm or deny whether records responsive to plaintiff's FOIA request exist. A *Glomar* response is appropriate where, as here, acknowledging whether responsive records exist would itself cause harm implicated by the FOIA's exemptions.

The district court properly entered summary judgment for NSA under Exemption 3, which exempts from disclosure matters specifically exempted by statute. The district court relied on Section 6 of the National Security Act, which provides that, "[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, [or] of any information with respect to the activities thereof[.]" As the courts have recognized, the terms of this provision are absolute, and they categorically exempt from disclosure *any* information regarding NSA's functions or activities.

As the NSA's declaration explains, either a positive or negative response to plaintiff's FOIA request would reveal information about NSA's Information Assurance mission, in which NSA is tasked with protecting national-security information systems. That mission includes monitoring commercial technologies used by the Government for security vulnerabilities, and gathering information from various sources about such security vulnerabilities or malicious attacks that pose a threat to Government information systems. As a result, if NSA were to disclose whether records responsive to plaintiff's FOIA request exist, that would reveal, *inter alia*, whether the cyber attack on Google was of concern to the United States for purposes of securing its national-security information systems; whether security vulnerabilities in Google technologies or applications were of concern to the United States; and whether the United States took any action in response to such concerns, including forming a partnership with or communicating with Google. Such information would plainly reveal NSA's functions and activities within the meaning of Section 6. Thus, the only recourse for NSA was to neither confirm nor deny whether responsive records exist. For that reason, the district court properly held that

the Government's declaration fully supports its *Glomar* response, and correctly entered summary judgment for NSA on that basis. The district court's decision, itself, provides a strong argument for affirmance.

Plaintiff EPIC's arguments to the contrary are without merit. Plaintiff's basic approach to the Government's substantial showing is to ignore it. Although plaintiff speculates that certain requested records might not reveal information about NSA's functions and activities, plaintiff too narrowly construes both the scope of Section 6 and NSA's Information Assurance mission.

Plaintiff further argues that this Court cannot properly review NSA's *Glomar* response because the Government failed to create a record for review by conducting a search. However, when an agency issues a *Glomar* response, the relevant record for review is the agency's declaration in support of non-disclosure. That record fully supports the NSA's *Glomar* response here.

Plaintiff also mistakenly urges this Court to reject the Government's *Glomar* response because of media reports allegedly confirming a partnership between Google and NSA, as well as NSA's own public acknowledgment of its Information Assurance mission. But media reports do not constitute official acknowledgment of information, and therefore cannot waive the agency's FOIA protection under Exemption 3. Nor does NSA's public acknowledgment of the existence of its

Information Assurance program require it to disclose details about that program that have not been previously disclosed by the agency and that are specifically exempted from disclosure by Section 6.

As this Court has noted, an agency's *Glomar* response must be upheld if it is supported by the record and not made in bad faith. The district court properly held that the Government's position here is amply supported by the NSA declaration, and no basis exists for concluding that it reflects any improper purpose. The district court thus properly upheld the Government's response, and its decision should be affirmed.

STANDARD OF REVIEW

This Court reviews *de novo* a district court's grant of summary judgment. *See Larson* v. *Department of State*, 565 F.3d 857, 862 (D.C. Cir. 2009).

ARGUMENT

I. THE DISTRICT COURT PROPERLY UPHELD THE GOVERNMENT'S *GLOMAR* RESPONSE.

A. A *Glomar* Response Is Appropriate When An Agency Can Neither Confirm Nor Deny The Existence of Requested Records Without Revealing Information That Is Exempt Under FOIA.

The FOIA generally mandates disclosure of Government records unless the requested information falls within an enumerated exemption. *See* 5 U.S.C. § 552(b). Notwithstanding the FOIA's "liberal congressional purpose," the statutory

exemptions must be given "meaningful reach and application." *John Doe Agency* v. *John Doe Corp.*, 493 U.S. 146, 152 (1989). "Requiring an agency to disclose exempt information is not authorized[.]" *Minier* v. *CIA*, 88 F.3d 796, 803 (9th Cir. 1996).

Agency decisions to withhold information under the FOIA are reviewed *de novo*, and the agency bears the burden of proving that the withheld information falls within the exemption it invokes. 5 U.S.C. § 552(a)(4)(B); *King* v. *Department of Justice*, 830 F.2d 210, 217 (D.C. Cir. 1987). Generally, an agency may meet its burden under FOIA by submitting a declaration that "describe[s] the justifications for nondisclosure with reasonably specific detail [and] demonstrate[s] that the information withheld logically falls within the claimed exemptions." *Hunt* v. *CIA*, 981 F.2d 1116, 1119 (9th Cir. 1992). A court may grant summary judgment to the government entirely on the basis of information set forth in such an affidavit, so long as the affidavit is "' not controverted by either contrary evidence in the record nor by evidence of agency bad faith.'" *Larson*, 565 F.3d at 862 (quoting *Miller* v. *Casey*, 730 F.2d 773, 776 (D.C. Cir. 1984)). "'Ultimately, an agency's justification for invoking a FOIA exemption is sufficient if it appears 'logical' or 'plausible.'" *Id.* (quoting *Wolf* v. *CIA*, 473 F.3d 370, 374-75 (D.C. Cir. 2007)).

The same standard applies when the Government issues a *Glomar* response, refusing to even acknowledge whether responsive records exist: in such

circumstances, the agency's affidavit must explain how the fact of the existence or non-existence of responsive records constitutes information protected by a FOIA exemption. *Phillipi* v. *CIA*, 546 F.2d 1009, 1013 (D.C. Cir. 1976); *Wolf*, 473 F.3d at 374 ("In determining whether the existence of agency records *vel non* fits a FOIA exemption, courts apply the general exception review standard established in non-*Glomar* cases.").

A *Glomar* response is appropriate where, as here, confirming or denying whether responsive records exist would itself cause the harm that a given FOIA exemption is intended to prevent. *See, e.g., Wilner* v. *NSA*, 592 F.3d 60, 68 (2d Cir. 2009) ("The *Glomar* doctrine is well settled as a proper response to a FOIA request because it is the only way in which an agency may assert that a particular FOIA statutory exemption covers the 'existence or nonexistence of the requested records' in a case in which a plaintiff seeks such records."), *cert. denied*, 131 S. Ct. 387 (2010); *Bassiouni* v. *CIA*, 392 F.3d 244, 246 (7th Cir. 2004) ("Every appellate court to address the issue has held that the FOIA permits the [agency] to make a '*Glomar* response' when it fears that inferences * * * or selective disclosure could reveal classified sources or methods of obtaining foreign intelligence."); *Minier*, 88 F.3d at 800 ("[A] government agency may issue a 'Glomar Response,' that is, refuse to confirm or deny the existence of certain records, if the FOIA exemption would itself

preclude the acknowledgment of such documents."); *Gardels* v. *CIA*, 689 F.2d 1100, 1103 (D.C. Cir. 1982) ("[A]n agency may refuse to confirm or deny the existence of records where to answer the FOIA inquiry would cause harm cognizable under an FOIA exception.").

In reviewing an agency's *Glomar* response, courts must be mindful when the information requested "implicat[es] national security, a uniquely executive purview." *Center for National Security Studies* v. *Department of Justice*, 331 F.3d 918, 926-27 (D.C. Cir. 2003). Indeed, the Supreme Court has cautioned that "weigh[ing] the variety of complex and subtle factors in determining whether disclosure of information may lead to an unacceptable risk of compromising" national security is a task best left to the Executive Branch. *CIA* v. *Sims*, 471 U.S. 159, 180 (1985); *see also Center for National Security Studies*, 331 F.3d at 928 ("[T]he 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.").

As a result, in the FOIA context, courts have "consistently deferred to executive affidavits predicting harm to the national security, and have found it unwise to undertake searching judicial review." *Center for National Security Studies*, 331

F.3d at 927; *see also Wilner*, 592 F.3d at 69 ("The '[a]ffidavits submitted by an agency are accorded a presumption of good faith."); *Students Against Genocide* v. *Department of State*, 257 F.3d 828, 840 (D.C. Cir. 2001) ("[S]ubstantial weight [is] owed to agency explanations in the context of national security, to qualify for withholding under Exemptions 1 and 3."); *Salisbury* v. *United States*, 690 F.2d 966, 970 (D.C. Cir. 1982) (noting that agencies possess "unique insights" into the adverse effects that might result from public disclosure of classified information); *Gardels*, 689 F.2d at 1104-05 ("Once satisfied that proper procedures have been followed and that the information logically falls into the exemption claimed, the courts 'need not go further to test the expertise of the agency, or to question its veracity when nothing appears to raise the issue of good faith.'").

B. The Government's *Glomar* Response Here Was Proper Under FOIA Exemption 3.

In reviewing an agency's invocation of FOIA Exemption 3, "the Supreme Court [has] engaged in a two-prong review. First, is the statute in question a statute of exemption as contemplated by exemption 3? Second, does the withheld material satisfy the criteria of the exemption statute?" *Fitzgibbon* v. *CIA*, 911 F.2d 755, 761-62 (D.C. Cir. 1990) (citing *Sims*, 471 U.S. at 167); *see also id.* ("'[T]he sole issue for decision is the existence of a relevant statute and the inclusion of withheld material

within the statute's coverage.'") (quoting *Association of Retired R.R. Workers* v. *United States R.R. Ret. Bd.*, 830 F.2d 331, 336 (D.C. Cir. 1987)). Because the answer to both of those questions is yes, this Court should uphold the district court's acceptance of NSA's *Glomar* response.

1. Here, NSA invoked Section 6 of the National Security Agency Act of 1959, Pub. L. No. 86-36, 73 Stat. 63, 64 (codified at 50 U.S.C. § 402 note), as the relevant statute of exemption for purposes of FOIA Exemption 3. Section 6 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 person employed by such agency.

Id.

As the district court correctly recognized, JA 111, this Court has already established that Section 6 "is a statute qualifying under Exemption 3." *Founding Church of Scientology* v. *NSA*, 610 F.2d 824, 828 (D.C. Cir. 1979); *accord Hayden* v. *NSA*, 608 F.2d 1381, 1389 (D.C. Cir. 1979); *see also Wilner*, 592 F.3d at 72. Indeed, plaintiff concedes as much. *See* Appellant's Opening Brief ("Br.") at 28. Accordingly, only the second prong of review is at issue in this appeal.

2. As explained in its affidavit, NSA determined that the records sought by plaintiff are protected by Section 6 and therefore properly withheld pursuant to FOIA

Exemption 3. That affidavit is sufficient to carry the agency's burden to justify its *Glomar* response here.

As courts have recognized, Section 6's coverage is quite broad, which "eases" the agency's burden in demonstrating that records are properly withheld. *Wilner*, 592 F.3d at 75 (noting "Congress's broad language in section 6"); *Larson*, 565 F.3d at 868 (NSA "need only demonstrate that the withheld information relates to the organization of the NSA or any function or activities of the agency"). Indeed, in enacting Section 6, Congress was "fully aware of the 'unique and sensitive activities of the [NSA],' which require 'extreme security measures.'" *Hayden*, 608 F.2d at 1390 (citing legislative history). For that reason, this Court has held that "[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). Moreover, because of the breadth of Section 6, "[a] specific showing of potential harm to national security * * * is irrelevant to the language of [Section 6]. Congress has already, in enacting the statute, decided that disclosure of NSA activities is potentially harmful." *Hayden*, 608 F.2d at 1390.

Particularly in light of the broad scope of Section 6, NSA reasonably concluded that acknowledging whether or not responsive records exist in this case would disclose information protected by that statutory provision. As explained in NSA's

declaration, one of NSA's primary cryptologic missions is its Information Assurance mission, under which NSA is tasked with protecting Government information systems and providing support to other agencies that protect the nation's critical infrastructure and key resources. JA 48. NSA fulfills that mission in part by discovering vulnerabilities in those information systems, monitoring malicious activity, and performing security testing. JA 48-49. Because the "government is largely dependent on commercial technology for its information systems," NSA also monitors commercial technologies purchased by the government for security vulnerabilities. JA 49. If such vulnerabilities in a commercial technology pose a threat to U.S. government information systems, NSA may take action against the threat. JA 49-50, 52.

As a result, if NSA were to disclose whether there are, or are not, records of a partnership or communications between Google and NSA regarding Google's security, that disclosure might reveal that NSA did or did not investigate the threat, that the threat was or was not of concern to the security of U.S. government information systems, and what measures NSA did or did not take in response. JA 52-53. The agency asserted that disclosure of such information would reveal NSA's functions and activities within the meaning of Section 6. JA 53. That judgment is owed "substantial weight." *Students Against Genocide*, 257 F.3d at 840.

Indeed, as the district court recognized with respect to the first category of records requested by plaintiff – records concerning an agreement between NSA and Google – NSA would only enter into an agreement with Google if NSA determined that any security vulnerability revealed by the January 2010 cyber attack poses potential harm to U.S. government information systems. JA 113; *see also* JA 52-53. Accordingly, acknowledging whether or not such records exist would reveal NSA's assessment of whether there is a security vulnerability that is of concern to the United States government. JA 52-53.

Similarly, as to the second and third categories of records requested by plaintiff – communications between NSA and Google regarding encryption of Gmail and cloud-based computing systems, such as Google Docs – NSA explained that it would only communicate with Google regarding Gmail or Google's use of encryption for cloud-based computing services such as Google Docs if NSA discovered a vulnerability in those commercial systems that posed a threat to U.S. government information systems. JA 52-53. To disclose whether any such records exist, therefore, would reveal protected information about NSA's functions and activities, including NSA's evaluation of potential cyber threats. *Id.*

Given the breadth of Section 6, the "logical and plausible" agency affidavit, JA 114, and the "substantial weight" owed to the agency's assessment about the risks of disclosure, the NSA's *Glomar* response was justified and must be upheld.

II. PLAINTIFF'S ARGUMENTS ARE MERITLESS.

Plaintiff does not dispute the agency's affidavit or allege bad faith. Instead, plaintiff's entire appeal is premised on the mistaken assumption that some of the records it seeks are not within Section 6's coverage, and are therefore not exempt under FOIA Exemption 3. It is clear from the face of plaintiff's FOIA request, however, that all of the requested records are exempt pursuant to FOIA Exemption 3 and Section 6.

A. Despite the breadth of Section 6 and NSA's explanation as to how plaintiff's FOIA request is encompassed by Section 6's coverage, EPIC speculates (Br. at 26, 28-29) that NSA might possess records that pertain only to *Google's* functions or activities, and that those records are therefore not exempt under Section 6. EPIC's understanding of both NSA's mission and Section 6's scope is too narrow. Even if plaintiff were correct that certain records or portions of records existed that revealed information only about Google (and nothing about NSA), those records, if maintained by the agency, would still constitute evidence of some kind of relationship between Google and NSA, formed in response to a potential security vulnerability or

malicious attack of concern to the United States. As NSA has explained, it is the relationship, not just the content or number of alleged records, that would reveal protected information about NSA's implementation of its Information Assurance mission. JA 53.

As the Janosek Declaration explains, NSA takes a "pro-active defense approach" in its protection of U.S. government information systems. JA 49. "This approach is dependent on information from a number of intelligence and open sources in order to have early awareness of potential malicious activity or vulnerabilities." *Id.* The specific types and identities of sources that NSA may choose to rely on are certainly a key aspect of its mission, and any information shedding light on such sources is protected by Section 6. For instance, NSA may gather information about potential security threats provided by private entities, which would be a protected activity under NSA's Information Assurance mission. If NSA did encourage and rely on reports of cybersecurity vulnerabilities from private entities such as Google, such a report, maintained in agency records, would be protected by Section 6, even though it might only concern Google's security vulnerabilities or Google's actions with respect to a particular security incident. Moreover, if such private entities knew that any such reports could be made public through a FOIA request, they might be hesitant to reach out to NSA, thereby hindering NSA's mission. These are precisely the

considerations Congress authorized NSA to take into account when it gave the agency broad power to protect information relating to its "function[s]" and "activities," § 6, 73 Stat. at 64; *see Hayden*, 608 F.2d at 1388 ("Congress intended reviewing courts to respect the expertise of an agency"), and NSA acted properly in making that determination in this case.

Plaintiff also suggests (Br. at 18) that some of the requested records, such as an unsolicited communication from Google, cannot be exempt under Section 6 and FOIA Exemption 3 because such a record "would not obviously cause any harm to the NSA's information assurance mission." But any suggestion that NSA is required to demonstrate harm to national security is mistaken. *Hayden*, 608 F.2d at 1390 ("A specific showing of potential harm to national security * * * is irrelevant to the language of Public Law No. 86-36. Congress has already, in enacting the statute, decided that disclosure of NSA activities is potentially harmful."). The only relevant question is whether, as a matter of law, the fact of the existence or nonexistence of responsive records "falls within the statute." *Larson*, 565 F.3d at 868. As explained above, Section 6 has an intentionally wide scope. And the information request at issue here plainly falls within that scope, and is thus categorically exempt from FOIA disclosure for that reason alone, without the need for any further showing. *Linder*, 94 F.3d at 698. In any event, as the district court correctly recognized, the Janosek

Declaration explains "the cognizable harm posed by acknowledging the existence/nonexistence of the information" at issue here. JA 114.

EPIC further speculates that "some records responsive to EPIC's FOIA Request concern NSA activities that may fall outside the scope of the agency's Section 6 authority," and are therefore not exempt. Br. at 26-27; *accord id.* at 30-31. For example, plaintiff contends (Br. at 30-31) that NSA is not authorized to enter into a collaborative agreement with Google regarding cybersecurity, and that such records are therefore not protected by Section 6. But insofar as Google's alleged communications or relationship with NSA provide information to NSA about potential threats to cyberspace, those communications would be relevant to NSA's function of securing government networks, and would therefore be protected under Section 6. In any event, plaintiff cannot challenge the merits of NSA's activities through a FOIA request. *See Wilner*, 592 F.3d at 76-77 (declining to address the legality of the Terrorist Surveillance Program as "beyond the scope of this FOIA action"); *Hrones* v. *CIA*, 685 F.2d 13, 19 (1st Cir. 1982) ("[Appellant] has chosen the wrong procedure for review of the legality of the operations of the agency. Such an investigation is not within the scope of court review of the denial of a FOIA request.").

B. Because plaintiff assumes there may be non-exempt records covered by its FOIA request, EPIC asserts that NSA was required to conduct a search for responsive records. *See* Br. at 10 (without a search, "not even the agency can know whether there is a factual basis for its legal position"); *accord id.* at 20-22. Plaintiff further contends that because NSA failed to conduct a search, it also failed to perform the requisite segregability analysis, *see* 5 U.S.C. § 552(b), to determine whether there was any non-exempt information that could be disclosed. Plaintiff's arguments demonstrate a fundamental misunderstanding of the purpose and consequences of a *Glomar* response.

When an agency issues a *Glomar* response, "the adequacy of the search is irrelevant * * * because the issue is whether the Agency has given sufficiently detailed and persuasive reasons for taking the position that it will neither confirm nor deny the existence or non-existence of any responsive records." *Wheeler* v. *CIA*, 271 F. Supp. 2d 132, 141-42 (D.D.C. 2003) (affirming a *Glomar* response when the agency "did not identify whether or to what extent it had conducted a search"); *see also Wolf*, 473 F.3d at 374 n.4 (rejecting plaintiff's argument that, to review the propriety of a *Glomar* response, the court must order the agency to search for responsive records). Indeed, particularly when a *Glomar* response is issued pursuant to Exemption 3, an agency may have no need to conduct a search. That is because

Exemption 3's "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." *Ass'n of Retired R.R. Workers*, 830 F.2d at 336.

In other words, it may be apparent from the face of a FOIA request that the existence or nonexistence of any responsive records falls within the scope of the relevant protective statute. Indeed, plaintiff concedes as much. Br. at 22 ("There may be times when a requested category of documents falls unquestionably within the gambit of a FOIA exemption."). That is particularly likely to be true when the applicable protective statute is as broad as Section 6. Moreover, when it is apparent from the face of a FOIA request that disclosure confirming or denying the existence of any responsive records is not required because of an expansive protective statute, conducting a search before issuing a *Glomar* response would be a meaningless (and costly) exercise.

That is precisely the circumstance presented by this case. As explained above, it is plain from the face of plaintiff's FOIA request that to confirm or deny the existence of responsive records would disclose information protected by Section 6. Specifically, NSA determined that responding to plaintiff's request might reveal whether NSA did or did not consider a particular cybersecurity incident, or security

settings in certain commercial technologies, to potentially expose U.S. government information systems to an external threat. JA 52-53. That threat assessment and any ensuing action or inaction would go to the heart of a major NSA function, its Information Assurance mission. JA 52-53. That well-supported determination alone fulfills NSA's obligation with respect to plaintiff's request. *Hayden*, 608 F.2d at 1390 ("[T]he Agency stated in its affidavit[] that all requested documents concerned a specific NSA activity * * * . This is all that is necessary for the Agency to meet its burden under Public Law No. 86-36 and Exemption 3.").

Plaintiff's reliance (Br. at 15-17, 22) on *Founding Church of Scientology* to suggest that NSA's affidavit is insufficient to supports its *Glomar* response is misplaced. This Court rejected the affidavit in that case as "far too conclusory" because the affidavit "furnishe[d] precious little that would enable a determination as to whether the materials withheld actually do bear on the agency's organization, functions or faculty for intelligence operations." 610 F.2d at 831; *id.* (the affidavit "merely states, without any elucidation whatever, that compliance with appellant's demand would reveal 'certain functions and activities * * * protected from mandatory disclosure by Section 6,' and would 'jeopardize national security functions the agency was established to perform.'") (citation omitted). In other words, the affidavit failed to describe "[h]ow agency functions might be unveiled," or which functions "might

be revealed." *Id.* In stark contrast, NSA's affidavit here expressly states which functions and activities would be implicated by disclosure, and how acknowledging the existence or non-existence of requested records would reveal those functions or activities.

EPIC incorrectly argues (Br. at 11, 25) that a search is also necessary to provide this Court with a record to review. But the Janosek Declaration, which explains why the records requested are exempt under Exemption 3 and Section 6, is the applicable record for this Court to review. *See Larson*, 565 F.3d at 869-70 (where the agency meets its burden by affidavit, and plaintiff points to no evidence of bad faith, there is no need for further record review); *Wolf*, 473 F.3d at 374 n.4 ("'When the agency's position is that it can neither confirm nor deny the existence of the requested records, there are no relevant documents for the court to examine other than the affidavits which explain the agency's refusal.'").

Plaintiff also contends (Br. at 22-26) that NSA's failure to conduct a search precluded it from making a segregability analysis, thereby invalidating the NSA's *Glomar* response. Plaintiff is mistaken. The Janosek Declaration expressly states that "acknowledgment of the existence or nonexistence of even one record or communication satisfying Plaintiff's request would improperly disclose a function or activity of NSA and could have negative effects on NSA's Information Assurance

mission." JA 53. Accordingly, NSA concluded that "there is no reasonably segregable, nonexempt portion of the requested records that can be released." *Id.* NSA, therefore, is entitled to a presumption that it complied with its obligation to disclose reasonably segregable material. *Sussman* v. *U.S. Marshals Service*, 494 F.3d 1106, 1117 (D.C. Cir. 2007).

In any event, a segregability analysis is required only when there are records, or portions of records, that are non-exempt. *See* 5 U.S.C. § 552(b) ("Any reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt under this subsection."). Where the NSA has already concluded that acknowledging the existence or non-existence of even one record would disclose information that is exempt, then *a fortiorari* there is no non-exempt information requiring a segregability analysis. *Cf. Wolf*, 473 F.3d at 374 n.4 (when agency invokes *Glomar* response, the only relevant documents for the court to review are the agency's affidavits).

C. Finally, plaintiff suggests that, because some information about NSA's Information Assurance mission is publicly available, NSA cannot legally refuse to confirm or deny the existence of records relating to that mission. *See* Br. at 18-19 (noting that "collaboration [between NSA and Google] was widely reported in the national media and acknowledged by the former director of the NSA"). Plaintiff's

argument is wide of the mark and, for that reason, the district court correctly rejected it. JA 112.

NSA has never officially acknowledged a collaborative relationship with Google – which is therefore purely a matter of theorization – and the national media is incapable of waiving NSA's statutory authority to protect information related to its functions and activities. Only official acknowledgment from "the agency from which the information is being sought" can waive an agency's protective power over records sought under FOIA,[2] *see Frugone* v. *CIA*, 169 F.3d 772, 774 (D.C. Cir. 1999); such waiver "cannot be based on mere public speculation, no matter how widespread." *Wolf*, 473 F.3d at 378; *see also Moore*, 2011 WL 6355313 at *3 ("'[a] strict test applies to claims of official disclosure'"); *ACLU* v. *DOD*, 628 F.3d 612, 621 (D.C. Cir. 2011) ("[W]e are hard pressed to understand the * * * contention that the release of a nongovernment document by a nonofficial source can constitute a disclosure affecting the applicability of the FOIA exemptions."). NSA has steadfastly refused

[2] Thus, EPIC's assertion (Br. at 6, 11, 19) that the *former* director of NSA has acknowledged a relationship between Google and NSA is irrelevant, as well as inaccurate. The former director simply acknowledged "[r]ecent reports of a *possible* partnership between Google and the government." Mike McConnell, *Mike McConnell on How to Win the Cyber-War We're Losing*, Wash. Post, Feb. 28, 2010, at B01 (emphasis added).

to confirm or deny the existence of any relationship with Google, and media reports do not affect its statutory authority to maintain that position.

Similarly, the fact that the existence of NSA's Information Assurance mission is public does not waive NSA's ability to protect the specific functions and activities that NSA undertakes in fulfilling that mission. Indeed, in *Wilner* the Second Circuit rejected the plaintiffs' argument that a *Glomar* response in that case, concerning the Terrorist Surveillance Program, was inappropriate because President Bush had already publicly confirmed the existence of that program. *Wilner*, 592 F.3d at 69-70 (holding that "an agency may invoke the *Glomar* doctrine in response to a FOIA request regarding a publicly revealed matter"). As that court concluded, the President's decision to make public the existence of an NSA intelligence-gathering program did not force the Government to reveal the program's most sensitive operational details. *Id.* at 69 ("The record is clear that * * * the specific methods used, targets of surveillance, and information obtained through the program have not been disclosed."). Thus, contrary to EPIC's premise here, it is settled under the FOIA that the fact that limited information regarding a clandestine activity has been released does not mean that all such information must therefore be released. *See Wilner*, 592 F.3d at 69-70; *Students Against Genocide*, 257 F.3d at 836; *Afshar* v. *Department of State*, 702 F.2d 1125, 1130-31 (D.C. Cir. 1983); *Salisbury*, 690 F.2d

at 971; *see also Fitzgibbon*, 911 F.2d at 766 ("[T]he fact that information resides in the public domain does not eliminate the possibility that further disclosures can cause harm to intelligence sources, methods, and operations.").

Nor does the fact that NSA makes certain "information about its information assurance mission available online," Br. at 19, waive NSA's ability to protect the information at issue here. Disclosure may be compelled over an agency's valid claim of exemption only where the specific information requested is the same information previously released through an authorized disclosure. *Moore*, 2011 WL 6355313 at *3; *Students Against Genocide*, 257 F.3d at 836; *Fitzgibbon*, 911 F.2d at 765. "As a consequence, 'a plaintiff asserting a claim of prior disclosure must bear the initial burden of pointing to specific information in the public domain that appears to duplicate that being withheld.'" *Wolf*, 473 F.3d at 378 (quoting *Afshar*, 702 F.32d at 1130). EPIC has failed to meet that burden. General security guidance provided to the public, including recommending the use of encryption when using Gmail, discloses nothing about NSA's specific functions and activities, including whether NSA has a relationship with Google.

CONCLUSION

For the foregoing reasons, the judgment of the district court should be affirmed.

Respectfully submitted,

TONY WEST
Assistant Attorney General

RONALD C. MACHEN, JR.
United States Attorney

DOUGLAS N. LETTER
(202) 514-3602

s/ Catherine Y. Hancock
CATHERINE Y. HANCOCK
(202) 514-3469
Attorneys, Appellate Staff
Civil Division, Room 7236
Department of Justice
Washington, D.C. 20530-0001

CERTIFICATE OF COMPLIANCE

Counsel for appellee hereby certifies that the foregoing Brief for Appellee satisfies the requirements of Federal Rule of Appellate Procedure 32(a)(7) and D.C. Circuit Rule 32(a). The brief was prepared in Times New Roman, 14-point font, and, excluding parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii) and D.C. Circuit Rule 32(a)(2), contains 7,263 words according to the count of Corel Wordperfect X5.

s/Catherine Y. Hancock
Catherine Y. Hancock
Counsel for Defendant-Appellee

CERTIFICATE OF SERVICE

I hereby certify that on January 26, 2012, I served the foregoing Brief for Appellee by causing an electronic copy to be served on the Court via the ECF system and eight paper copies via hand delivery, and by causing one copy to be served on the following counsel via the ECF system:

Marc Rotenberg
John Arthur Verdi
Electronic Privacy Information Center
1718 Connecticut Avenue, NW
Suite 200
Washington, D.C. 20009
(202) 483-1140

s/Catherine Y. Hancock
Catherine Y. Hancock
Counsel for Defendant-Appellee

STATUTORY ADDENDUM

5 U.S.C. § 552(b)(3):

(b) This section does not apply to matters that are--

* * *

(3) specifically exempted from disclosure by statute (other than section 552b of this title), if that statute--

(A)(i) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue; or

(ii) establishes particular criteria for withholding or refers to particular types of matters to be withheld; and

(B) if enacted after the date of enactment of the OPEN FOIA Act of 2009, specifically cites to this paragraph.

National Security Agency Act of 1959, § 6, Pub. L. No. 86-36, 73 Stat. 63, 64 (1959) (codified at 50 U.S.C. § 402 note):

Sec. 6. (a) Except as provided in subsection (b) of this section, nothing in this Act or any other law (including, but not limited to, the first section and section 2 of the Act of August 28, 1935 (5 U.S.C. 654)) [repealed by Pub.L. 86-626, Title I, § 101, July 12, 1960, 74 Stat. 427] 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 the persons employed by such agency.

(b) The reporting requirements of section 1582 of title 10, United States Code, shall apply to positions established in the National Security Agency in the manner provided by section 4 of this Act.