

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA**

---

ELECTRONIC PRIVACY  
INFORMATION CENTER,

Plaintiff,

v.

DEPARTMENT OF HOMELAND  
SECURITY,

Defendant.

---

Case No. 1:13-CV-260 (JEB)

**MOTION FOR SUMMARY JUDGMENT**

Defendant hereby moves for summary judgment under Federal Rule of Civil Procedure 56. The bases for this motion are explained in the accompanying memorandum.

Dated: June 28, 2013

Respectfully submitted,

STUART F. DELERY  
Acting Assistant Attorney General

RONALD C. MACHEN JR  
United States Attorney

ELIZABETH J. SHAPIRO  
Deputy Director, Federal Programs  
Branch, Civil Division

/s/ Justin M. Sandberg  
JUSTIN M. SANDBERG  
(Ill. Bar No. 6278377)  
Trial Attorney  
U.S. Dept. of Justice, Civil Division,  
Federal Programs Branch

20 Mass. Ave., NW, Rm. 7302  
Washington, DC 20001  
(202) 514-5838 phone  
(202) 616-8202 fax  
justin.sandberg@usdoj.gov

Attorneys for Defendant

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA**

ELECTRONIC PRIVACY  
INFORMATION CENTER,

Plaintiff,

v.

DEPARTMENT OF HOMELAND  
SECURITY,

Defendant.

Case No. 1:13-CV-260 (JEB)

**MEMORANDUM IN SUPPORT OF SUMMARY JUDGMENT**

**INTRODUCTION**

Plaintiff Electronic Privacy Information Center (EPIC) has sued the Department of Homeland Security (DHS) under the Freedom of Information Act (FOIA), 5 U.S.C. § 552. This suit stems from EPIC’s request for records detailing a process for shutting down wireless networks to prevent, among other things, the remote detonation of bombs. The complaint raises three claims, but one – based on DHS’s alleged failure to meet statutory deadlines, Compl. ¶¶ 39-42 – has been rendered moot by the filing of this motion. *See Atkins v. Dep’t of Justice*, 1991 WL 185084, at \*1 (D.C. Cir. Sept. 18, 1991); *Muttitt v. Dep’t of State*, 2013 WL 781709, \*9 (D.D.C. March 4, 2013). The remaining claims raise two basic questions: (1) did the agency conduct an adequate search; and (2) did the agency properly withhold any responsive documents that are subject to the FOIA. The answer to both questions is “yes.” The agency conducted an adequate search – it located the only document subject to the FOIA that is responsive to EPIC’s

request – and has properly withheld portions of that document under Exemptions 6, 7(C), 7(E), 7(F).

As DHS located the sole document responsive to the FOIA request, EPIC's challenge to the sufficiency of the search should be dismissed as moot. In the alternative, the Court should enter judgment in DHS's favor because it conducted a search reasonably calculated to locate responsive records. The Court should also enter judgment in DHS's favor with respect to its decision to withhold the document in part.<sup>1</sup>

### **FACTUAL AND PROCEDURAL BACKGROUND**

EPIC submitted a FOIA request to DHS seeking three specific categories of records:

- 1) The full text of Standard Operating Procedure 303;
- 2) The full text of the pre-determined 'series of questions' that determines if a shutdown is necessary; [and]
- 3) Any executing protocols or guidelines related to the implementation of Standard Operating Procedure 303, distributed to DHS, other federal agencies, or private companies, including protocols related to oversight of shutdown determinations.

EPIC FOIA Request, July 10, 2012, at 3 (attached as Ex. 1). Generally speaking, Standard Operating Procedure (SOP) 303 describes a “shutdown and restoration process for use by commercial and private wireless networks during national crisis.” *Id.* (quoting the National Security Telecommunications Advisory Committee [NSTAC], NSTAC Issue Review 2006-07 at 139 (2007) available at <http://www.ncs.gov/nstac/reports/2007/2006-2007%20NSTAC%20Issue%20Review.pdf>). More specifically, SOP 303 details a process for the “deactivation of wireless networks” to “deter the triggering of radio-activated improvised explosive devices.” Declaration of James V.M.L. Holzer, Senior Director of FOIA Operations for the DHS Privacy Office, June 28, 2013, ¶ 25 (attached as Ex. 2).

---

<sup>1</sup> DHS is providing EPIC with the non-exempt portions of the record today.

DHS conducted a search for responsive documents subject to the FOIA but initially located none. Letter from Mia Day, DHS FOIA Program Specialist, to Amie L. Stepanovich, Assoc. Litigation Counsel, EPIC, Aug. 21, 2012 (attached as Ex. 3). (These searches are described below and in the in the attached Holzer Declaration.) EPIC appealed the agency's determination that there were no responsive documents subject to the FOIA, arguing that DHS had failed to perform an adequate search. EPIC Admin. Appeal, Sept. 13, 2012 (attached as Ex. 4). On appeal, the Office of the Chief Administrative Law Judge for the U.S. Coast Guard, which handles certain FOIA appeals for DHS, concluded that DHS had not sufficiently demonstrated the adequacy of its search. Decision Letter from Joanna Sherry, Attorney Advisor, Office of the Chief ALJ, to Stepanovich, March 25, 2013, at 1 (attached as Ex. 5). The matter was remanded to the agency for further review. *Id.* After this administrative remand, DHS conducted additional searches. The agency located the only responsive document subject to the FOIA – a copy of SOP 303. Holzer Decl. ¶¶ 19, 21. DHS is withholding large portions of this document under FOIA Exemptions 7(E) and 7(F), and smaller segments under Exemptions 6 and 7(C).

### **STANDARD OF REVIEW**

Summary judgment is appropriate when there is no genuine issue as to any material fact and the moving party is entitled to judgment as a matter of law. *See* Fed. R. Civ. P. 56(a); *Diamond v. Atwood*, 43 F.3d 1538, 1540 (D.C. Cir. 1995). FOIA actions are typically resolved on summary judgment. *Reliant Energy Power Generation, Inc. v. FERC*, 520 F. Supp. 2d 194, 200 (D.D.C. 2007). With respect to a claim regarding the adequacy of a search, a court may enter summary judgment based solely on information in an agency declaration when it describes in reasonable detail a search reasonably calculated to uncover all

relevant documents. *Thornton-Bey v. Exec. Office for U.S. Attorneys*, 844 F. Supp. 2d 159, 163 (D.D.C. 2012). With regard to exemption claims, an agency declaration suffices when the declaration describes “the documents and the justifications for nondisclosure with reasonably specific detail, demonstrate[s] that the information withheld logically falls within the claimed exemption, and [is] not controverted by either contrary evidence in the record [ ] or by evidence of agency bad faith.” *Military Audit Project v. Casey*, 656 F.2d 724, 738 (D.C. Cir. 1981). Agency declarations are “accorded a presumption of good faith, which cannot be rebutted by purely speculative claims about the existence and discoverability of other documents.” *SafeCard Servs., Inc. v. SEC*, 926 F.2d 1197, 1200 (D.C. Cir. 1991) (quotation marks omitted).

## **ARGUMENT**

### **I. DHS Performed A Search Reasonably Calculated to Discover Responsive Documents**

On summary judgment in a FOIA case, the agency must demonstrate that it has conducted an adequate search. To do so, it must explain the “scope and method of the search” in “reasonable detail[,]” but need not provide “meticulous documentation [of] the details of an epic search.” *Perry v. Block*, 684 F.2d 121, 127 (D.C. Cir. 1982). The agency must show “that it made a good faith effort to conduct a search for the requested records, using methods which can be reasonably expected to produce the information requested.” *Oglesby v. U.S. Dep’t of the Army*, 920 F.2d 57, 68 (D.C. Cir. 1990). “There is no requirement that an agency search every record system.” *Id.* Moreover, “the issue to be resolved is not whether there might exist any other documents possibly responsive to the request, but rather whether the *search* for those documents was *adequate*.” *Weisberg v. Dep’t of Justice*, 745 F.2d 1476, 1485 (D.C. Cir. 1984) (italics in original); *see also Yelder v. Dep’t of Defense*, 577 F. Supp. 2d 342, 344-46 (D.D.C. 2008). “[A] search need not be

perfect, only adequate, and adequacy is measured by the reasonableness of the effort in light of the specific request.” *Meeropol v. Meese*, 790 F.2d 942, 956 (D.C. Cir. 1986). Conducting a “reasonable” search is a process that requires “both systemic and case specific exercises of discretion and administrative judgment and expertise.” *Schrecker v. Dep’t of Justice*, 349 F.3d 657, 662 (D.C. Cir. 2003) (quoting *Johnson v. Exec. Office for U.S. Attorneys*, 310 F.3d 771, 776 (D.C. Cir. 2002)).

As a threshold matter, EPIC’s challenge to the sufficiency of the search is moot. A plaintiff must establish that the court has jurisdiction over each claim. *See DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 352-54 (2006). A claim is moot if there is no meaningful relief that a court can grant. *United States v. Garde*, 848 F.2d 1307, 1309 (D.C. Cir. 1988). Other than ordering DHS to more specifically describe the search that it already conducted, the only relief that the Court could grant to EPIC with regard to its sufficiency-of-the-search claim would be an order remanding the case to the agency and instructing it to perform a reasonable search. *See People for the Ethical Treatment of Animals, Inc. v. Bureau of Indian Affairs*, 800 F. Supp. 2d 173, 178 n. 2 (D.D.C. 2011). But such an order would not provide meaningful relief here because DHS has already located the only information sought by EPIC. EPIC sought only SOP 303 and the two closely related categories of implementing documents (*i.e.*, those containing the full text of the authentication questions and any executing protocols). EPIC FOIA Request at 3 (attached as Ex. 1). It did not seek drafts of these documents, internal emails discussing these documents, or anything else. *See id.* DHS located SOP 303, which contains all three categories of records sought by EPIC. As the Holzer declaration explains, the component of DHS that authored the document, and which implements it, stated that “there are no other documents that contain either the full text of the questions or any executing protocols or guidelines.” Holzer

Decl. ¶ 19. Thus, DHS found the documents requested by EPIC, there is nothing left to search for, and the claim is moot.

In any case, DHS performed a search reasonably calculated to produce the information requested. Upon receiving the FOIA request, DHS's Privacy Office, which directs the agency's FOIA operation, contacted the four components of the agency most likely to have responsive records: (1) the DHS Management Directorate, (2) the Office of the Chief Information Officer (OCIO), (3) the Under Secretary for Management, and (4) the National Protection and Programs Directorate (NPPD). Holzer Decl. ¶¶ 10, 12. The Management Directorate and the Under Secretary's offices were contacted because each office has a "broad portfolio" of responsibilities and, consequently, "often will know about a policy, procedure or initiative." *Id.* ¶¶ 12, 13. The Privacy Office contacted the OCIO because the request related to communications and that office "is often involved in, and consulted on, information and communication issues." *Id.* ¶ 13. Finally, the Privacy Office contacted the NPPD because the FOIA request specifically mentioned a former organization within the NPPD, namely, the National Communications System, and a current organization within the NPPD, the National Coordinating Center for Communications. *Id.* ¶10; EPIC FOIA Request at 1 (attached as Ex. 1).

The Management Directorate, the OCIO, and the Under Secretary's office each conducted searches for responsive records. "These offices do not have one database to search for records that are responsive to [FOIA] . . . requests." Holzer Decl. ¶ 15. Thus, each searched "shared computer drives, Share Point sites, and emails for information about the requested records." *Id.* As the declaration explains, "[t]hese are the storage places where DHS employees would typically place information about the products they are working on as well as copies of any final products . . . ." *Id.* They searched using the search terms "Standard Operating



Procedure 303” and “SOP 303.” *Id.* None of the offices located a record subject to the FOIA responsive to EPIC’s request. *Id.* ¶ 16.

The NPPD initially declined to search, stating that it had no records responsive to the request. Holzer Decl. ¶ 11. After the ALJ remanded the matter to the agency in response to EPIC’s administrative appeal, the Privacy Office again approached the NPPD. *Id.* ¶ 19. At that time, the NPPD recognized that it had erred in responding to the Privacy Office’s initial inquiry: The NPPD had confused the documents sought by EPIC’s request with those sought in a different, but similar, request submitted by another party. *Id.* ¶ 11. The NPPD then searched and located a copy of SOP 303. *Id.* ¶ 19. It also recognized that SOP 303 contained all three categories of information sought by EPIC, and that no other document contained these narrow categories of information. *Id.* ¶¶ 19, 21.

This description of the search, along with the additional details included in the declaration, establish that DHS conducted a search reasonably calculated to locate the information requested. The Holzer declaration identifies the DHS components most likely to have responsive material; the reason those components were likely to have responsive material; the general processes employed in conducting the search for documents, including the search terms used; and the record located – the SOP. The declaration also explains that DHS concluded its search after locating the SOP because it is the only potentially responsive record; no other records contain the narrow categories of information sought by plaintiff. Concluding the search at that point was reasonable because “the reasonableness of an agency’s search [is] based on what the agency knew at its conclusion rather than what the agency speculated at its inception,” *Campbell v. U.S. Dep’t of Justice*, 164 F.3d 20, 28 (D.C. Cir. 1998), and at the conclusion, the agency knew that it had the SOP and that “are no other documents that contain the full text of the

questions or any executing protocols,” Holzer Decl. ¶ 21. Thus, Mr. Holzer’s declaration provides “in reasonable detail the scope and method of the search conducted by the agency [and] will suffice to demonstrate compliance” with FOIA. *Perry*, 684 F.2d at 127. DHS, through its various components, “made a good faith effort to search for the records requested,” and “its methods were reasonably expected to produce the information requested,” *Kidd v. Dep’t of Justice*, 362 F. Supp. 2d 291, 294 (D.D.C. 2005) (internal quotations and citation omitted).

## **II. SOP 303 Is Exempt, in Part, from Disclosure**

### **A. Exemption 7(E) Shields the Document Sought From Disclosure**

DHS has properly withheld SOP 303 in part because releasing the withheld portions would reveal a technique for law enforcement, specifically, for preventing the use of wireless networks to detonate bombs that would endanger persons and/or property.<sup>2</sup>

Exemption 7 applies to records “compiled for law enforcement purposes.” 5 U.S.C. § 552(b)(7). “But it exempts such documents from disclosure only to the extent that production of the information might be expected to produce one of six specified harms.” *Keys v. U.S. Dep’t of Justice*, 830 F.2d 337, 340 (D.C. Cir. 1987). The FOIA lists the harms in discrete subsections. Subsection 7(E) exempts documents or information that “would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.” 5 U.S.C. § 552(b)(7)(E). In short, this is a two-part inquiry: DHS must “demonstrate[ ] both the threshold law enforcement purpose and the danger that at

---

<sup>2</sup> Count III of the complaint could be read to suggest that EPIC is entitled to summary judgment because DHS did not meet statutorily imposed deadlines. Even if DHS failed to meet the deadlines, this suggestion is wrong. *Landmark Legal Found. v. EPA*, 272 F. Supp. 2d 59, 68 (D.D.C. 2003) (“[A] lack of timeliness or compliance with FOIA deadlines does not preclude summary judgment for an agency, nor mandate summary judgment for the requester.”).

least one of the specified harms [– here, the one identified in 7(E) –] would flow from disclosure.” *Keys*, 830 F.2d at 340. DHS satisfies this burden.

To establish the first part of the inquiry, *i.e.*, that the document was compiled for law enforcement purposes, DHS need only make a colorable claim that there is a rational “nexus between the agency’s activity” underlying the creation of the document and the agency’s “law enforcement duties.” *Id.*; *see also Tax Analysts v. IRS*, 294 F.3d 71, 76-79 (D.C. Cir. 2002). The range of law enforcement purposes falling within the scope of Exemption 7 includes law enforcement activities designed to prevent crimes and terrorist attacks: “[S]teps by law enforcement officers to prevent terrorism surely fulfill ‘law enforcement purposes,’” *Milner v. Dep’t of Navy*, 131 S.Ct. 1259, 1272 (2011) (Alito, J., concurring); *see also Pratt v. Webster*, 673 F.2d 408, 421 (D.C. Cir. 1982) (including “the maintenance of national security” as a law enforcement purpose); *Pub. Emp. for Envtl. Responsibility v. U.S. Section Int’l Boundary and Water Comm’n*, 839 F.Supp.2d 304, 327 (D.D.C. 2012) (shielding plans for responding to dam failures); *U.S. News & World Report v. Dep’t of the Treasury*, No. 84-2303, 1986 U.S. Dist. LEXIS 27634, at \*5 (D.D.C. Mar. 26, 1986) (protecting Secret Service’s contract specifications for President’s armored limousine); *Living Rivers, Inc. v. U.S. Bureau of Reclamation*, 272 F. Supp. 2d 1313, 1318-20 (D. Utah 2003) (exempting from disclosure inundation maps, which show the effect of dam failure); *Asian Law Caucus v. DHS*, No. 08-00842, 2008 WL 5047839, at \*4 (N.D. Cal. Nov. 24, 2008) (protecting from disclosure documents with details about terrorism watch lists); *Gordon v. FBI*, 388 F. Supp. 2d 1028, 1035-36 (N.D. Cal. 2005) (same); *Judicial Watch, Inc. v. U.S. Dep’t of Commerce*, 337 F. Supp. 2d 146, 181-82 (D.D.C. 2004) (approving withholding of “firearm specifications” and “radio frequencies” used by agents protecting Secretary of Commerce); *Voinche v. FBI*, 940 F. Supp. 323, 329, 332 (D.D.C. 1996) (allowing

the withholding of documents regarding the Supreme Court’s security measures). This makes sense because “[t]he ordinary understanding of law enforcement includes not just the investigation and prosecution of offenses that have already been committed, but also proactive steps designed to prevent criminal activity and to maintain security.” *Milner*, 131 S. Ct. at 1272 (Alito, J., concurring).

What is more, courts defer to a law enforcement agency’s assertion that information or documents were compiled for a law enforcement purpose because government agencies “typically go about their intended business.” *Pratt*, 673 F.2d at 417-18. And “DHS . . . [is] unquestionably [a] federal law enforcement agenc[y].” *Nat’l Day Laborer Organizing Network v. U.S. Immigration & Customs Enforcement Agency*, 811 F. Supp. 2d 713, 744-45 (S.D.N.Y. 2011).

DHS compiled SOP 303 for a law enforcement purpose. Holzer Decl. ¶ 20 (“The SOP was compiled for a law enforcement purpose . . .”). SOP 303, which was drafted by a component of DHS, is “a homeland security procedure primarily intended to efficiently and effectively deter the triggering of radio-activated improvised explosive devices . . . that would endanger life and property.” Holzer Decl. ¶¶ 20, 25. As established by the numerous cases cited above, efforts to prevent terrorism, like the one enshrined in SOP, constitute an essential law enforcement activity. Indeed, “[p]articularly in recent years, terrorism prevention and national security measures have been recognized as vital to effective law enforcement efforts in our Nation.” *Milner*, 131 S. Ct. at 1272 (Alito, J., concurring). And there is a self-evidently rational “nexus” between this activity – *i.e.*, instituting a process for shutting down wireless networks to prevent bombings – and the Department of *Homeland Security*’s law enforcement duties: DHS exists to keep the country safe and preventing bombings does just that. *See Keys*, 830 F.2d at

340. Finally, even if there were some doubt about whether DHS compiled SOP 303 for a law enforcement purposes (there is not), that doubt would be resolved in DHS's favor given that it is a law enforcement agency. *See Pratt*, 673 F.2d at 417-18. Thus, DHS has made the threshold showing for invoking Exemption 7 by demonstrating that SOP 303 was "compiled for law enforcement purposes." 5 U.S.C. § 552(b)(7). The inquiry, then, moves to step two, establishing the existence of the harm described in subsection 7(E).

Exemption 7(E) protects law-enforcement documents that "would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law." 5 U.S.C. § 552(b)(7)(E). Exemption 7(E) protects from disclosure techniques and procedures used to prevent and protect against crimes, as well as techniques and procedures used to investigate crimes after they have been committed. *See, e.g., U.S. News & World Report*, 1986 U.S. Dist. LEXIS 27634, at \*5-6. Exemption 7(E) does not require a particular determination of harm that would result from disclosure of specific records or information; rather, the exemption categorically protects information related to law enforcement techniques. *See Smith v. Bureau of Alcohol, Tobacco & Firearms*, 977 F. Supp. 496, 501 (D.D.C. 1997) ("Exemption 7(E) provides categorical protection to information related to law enforcement techniques."); *Fisher v. Dep't of Justice*, 772 F. Supp. 7, 12 n.9 (D.D.C. 1991), *aff'd*, 968 F.2d 92 (D.C. Cir. 1992).

Releasing SOP 303 would result in the disclosure of a law enforcement technique. The technique at issue here is DHS's technique for coordinating an orderly process for disabling a wireless telecommunications network to prevent, among other things, the use of the network to remotely detonate an explosive device. Holzer Decl. ¶ 25. "SOP 303 establishes a protocol for

verifying that circumstances exist that would justify shutting down wireless networks . . . [and] provides a step-by-step process for the orderly shut-down of wireless networks following verification of the facts and appropriate weighing of the circumstances.” *Id.* This is undoubtedly a technique, *i.e.*, a “procedure” or “a particular way of doing or of going about the accomplishment of something.” *See Webster's Third New International Dictionary* (1986). And while such a technique might not fit within some crabbed notions of law enforcement techniques, “[i]t is inconceivable . . . that Congress meant to afford [preventative law enforcement] activities any less protection from disclosure simply because they do not fit within the traditional notion of investigative law enforcement techniques. Indeed, it is difficult to imagine agency procedures or techniques more deserving of protection.” *U.S. News & World Report*, 1986 U.S. Dist. LEXIS 27634, at \*6-7.

**B. DHS Has Properly Withheld SOP 303 Under Exemption 7(F)**

DHS has withheld portions of SOP 303 under Exemption 7(F) because releasing them, and thereby disclosing portions of the process for shutting down wireless networks to prevent bombings, could endanger individuals’ physical safety.

Exemption 7(F) shields from disclosure records or information compiled for a law enforcement purpose, if its production “could reasonably be expected to endanger the life or physical safety of any individual.” 5 U.S.C. § 552(b)(7)(F). “While courts generally have applied Exemption 7(F) to protect law enforcement personnel or other specified third parties, by its terms, the exemption is not so limited; it may be invoked to protect ‘any individual’ reasonably at risk of harm.” *Amuso v. U.S. Dept. of Justice*, 600 F. Supp. 2d 78, 101 (D.D.C. 2009) (quotation marks omitted). Indeed, in *Living Rivers*, the court upheld the Bureau of Reclamation’s invocation of Exemption 7(F) over inundation maps, which described the effects

of dam failures for the areas downstream from the Hoover and Glen Canyon Dams, because those maps could be used to aid terrorist attacks on the dams that would jeopardize the downstream population. 272 F. Supp. 2d at 1321-22. Importantly, “[w]ithin limits, the Court[s] defer[ ] to [an] agency’s assessment of danger.” *Amuso*, 600 F. Supp. at 101.

DHS properly withheld SOP 303 because its disclosure could reasonably be expected to endanger the physical safety of individuals near unexploded bombs. DHS has already established that it compiled SOP 303 for law enforcement purposes. *See* § II.A above. Thus, it need only demonstrate that releasing SOP 303 could reasonably be expected to endanger the physical safety of any individual. 5 U.S.C. § 552(b)(7). SOP 303 describes a procedure for shutting down wireless networks to prevent bombings that would endanger lives. Holzer Decl. ¶ 25. Releasing information regarding this protocol would enable “bad actors” to blunt its usefulness, perhaps even by insinuating themselves into the process. *Id.* ¶ 26. Neutering this protocol could reasonably be expected to endanger the physical safety of those near a bomb by increasing the chances that the process will fail and the bomb will explode. “Given that disclosure of the requested information could reasonably lead to circumvention of or interference with a procedure aimed at preventing the triggering of improvised explosive devices, there is a reasonable expectation that disclosure could reasonably endanger the lives or physical safety of the general public.” *Id.* This assessment of danger by DHS, a law enforcement agency, is eminently reasonable and deserving of deference. *See Amuso*, 600 F. Supp. at 101.

#### C. DHS Properly Withheld Information in SOP 303 Under Exemption 7(C) and Exemption 6

DHS has withheld from the disclosure the names, direct-dial telephone numbers, and email addresses of state homeland security officials to protect their personal privacy. Holzer Decl. ¶¶ 23-24. These withholdings are justified under Exemptions 6 and 7(C).

Exemption 7(C) protects records or information compiled for a law enforcement purpose to the extent that the production of records “could reasonably be expected to constitute an unwarranted invasion of personal privacy.” 5 U.S.C. § 552(b)(7)(C). Exemption 6 protects “personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.” 5 U.S.C. § 552(b)(6). The D.C. Circuit has interpreted the term “files” in the context of Exemption 6 to encompass “not just files, but also bits of personal information, such as names and addresses, the release of which would create a palpable threat to privacy.” *Judicial Watch v. FDA*, 449 F.3d 141, 152-53 (D.C. Cir. 2006). Both exemptions require the agency and the court to “balance the privacy interests that would be compromised by disclosure against the public interest in release of the requested information.” *Beck v. Dep’t of Justice*, 997 F.2d 1489, 1491 (D.C. Cir. 1993). The only relevant public interest is the interest in knowing what the government is up to. *Sussman v. U.S. Marshals Svc.*, 494 F.3d 1106, 1115 (D.C. Cir. 2007); *Nat’l Ass’n of Home Bldgs. v. Norton*, 309 F.3d 26, 34 (D.C. Cir. 2002).

Though both exemptions require balancing, “the balance tilts more strongly toward nondisclosure in the context of Exemption 7(C) because Exemption 7(C)’s privacy language is broader than the comparable language in Exemption 6 in two respects.” *Braga v. FBI*, 2012 WL 6644356, at \*5 (D.D.C. Dec. 21, 2012) (quotation marks omitted). First, Exemption 6 protects files that, if released, would result in a “clearly unwarranted invasion of personal privacy”; Exemption 7 omits the word “clearly.” *Id.* Second, Exemption 7 covers documents that, if released, “could reasonably be expected to constitute” an invasion of privacy, while Exemption 6 covers documents that “would constitute” an invasion of privacy. *Id.*



The differences in these standards are irrelevant here, however, as DHS's withholding satisfies both exemptions.<sup>3</sup> Releasing the names, direct-dial telephone numbers, and email addresses of state homeland security officials would invade their personal privacy by subjecting them to possible harassment, as well as targeting by bad actors. Holzer Decl. ¶¶ 23, 24; *see Lazaridis v. U.S. Dep't of State*, 2013 WL 1226607, at \*12 (D.D.C. March 27, 2013) (Exemption 7); *Judicial Watch*, 449 F.3d at 152-53 (Exemption 6); *Nat'l Right to Work Legal Defense & Education Fund v. U.S. Dep't of Labor*, 828 F. Supp. 2d 183, 192-93 (D.D.C. 2011) (Exemption 6). And there is no public interest in the release of this information, as it does not provide information about what the government is up to. *See* Holzer Decl. ¶¶ 23, 24; *Lazaridis*, 2013 WL 1226607, at \*12 (Exemption 7(C)) ; *Nat'l Right to Work*, 828 F. Supp. 2d at 192-93 (Exemption 6). Thus, these withholdings are proper. *See Sussman*, 494 F.3d at 1115 (Exemption 7(c)); *Lazaridis*, 2013 WL 1226607, at \*12 (Exemption 7(C)) ; *Nat'l Right to Work*, 828 F. Supp. 2d at 192-93 (Exemption 6).

### **III. The Agency Performed an Appropriate Segregability Analysis**

The agency carefully reviewed SOP 303 and determined that portions of SOP 303 could be separated from the exempt sections of the documents and released. Those non-exempt portions are being provided to EPIC. No other segments of the document could be released without compromising the interests protected by the exemptions invoked by DHS. Holzer Decl. ¶ 22.

---

<sup>3</sup> As discussed before, DHS has demonstrated that it compiled SOP 303 for law enforcement purposes).

**CONCLUSION**

The Court should dismiss EPIC's adequacy-of-the-search claim as moot and enter judgment in favor of DHS with regard to EPIC's challenge to the agency's withholding. In the alternative, the Court should enter judgment in favor of DHS with respect to all claims.

Dated: June 28, 2013

Respectfully submitted,

STUART F. DELERY  
Acting Assistant Attorney General

RONALD C. MACHEN JR  
United States Attorney

ELIZABETH J. SHAPIRO  
Deputy Director, Federal Programs Branch,  
Civil Division

/s/ Justin M. Sandberg  
JUSTIN M. SANDBERG  
(Ill. Bar No. 6278377)  
Trial Attorney  
U.S. Dept. of Justice, Civil Division,  
Federal Programs Branch  
20 Mass. Ave., NW, Rm. 7302  
Washington, DC 20001  
(202) 514-5838 phone  
(202) 616-8202 fax  
justin.sandberg@usdoj.gov

Attorneys for Defendant

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA**

---

ELECTRONIC PRIVACY  
INFORMATION CENTER,

Plaintiff,

v.

DEPARTMENT OF HOMELAND  
SECURITY,

Defendant.

---

Case No. 1:13-CV-260 (JEB)

**DEFENDANT’S STATEMENT OF UNDISPUTED MATERIAL  
FACTS IN SUPPORT OF MOTION FOR SUMMARY JUDGMENT**

Pursuant to Local Civil Rule 7(h), Defendants submit this statement of material facts as to which no genuine issue exists.

1. Plaintiff Electronic Privacy Information Center (EPIC) submitted a Freedom of Information Act (FOIA) request to the Department of Homeland Security (DHS) seeking three categories of records:

- 1) The full text of Standard Operating Procedure 303;
- 2) The full text of the pre-determined ‘series of questions’ that determines if a shutdown is necessary; [and]
- 3) Any executing protocols or guidelines related to the implementation of Standard Operating Procedure 303, distributed to DHS, other federal agencies, or private companies, including protocols related to oversight of shutdown determinations.

EPIC FOIA Request, July 10, 2012 (attached as Ex. 1).

2. Standard Operating Procedure (SOP) 303 is a document that details a process for the “deactivation of wireless networks” primarily to “deter the triggering of radio-

activated improvised explosive devices.” Declaration of James V.M.L. Holzer, Senior Director of FOIA Operations for the DHS Privacy Office, June 28, 2013, ¶ 25 (attached as Ex. 2).

3. Upon receiving the FOIA request, DHS’s Privacy Office contacted the components of the agency most likely to have responsive records: (1) the DHS Management Directorate, (2) the Office of the Chief Information Officer (OCIO), (3) the Under Secretary for Management, and (4) the National Protection and Programs Directorate (NPPD). *Id.* ¶¶ 10, 12.
4. The Privacy Office asked these components to search their files for responsive records. *Id.* ¶¶ 10, 12.
5. The Management Directorate and the Under Secretary’s offices were asked to search their records because each office has a “broad portfolio” of responsibilities and, consequently, “often will know about a policy, procedure or initiative.” *Id.* ¶¶ 12, 13.
6. The OCIO was asked to search its records because the request related to communications and that office “is often involved in, and consulted on, information and communication issues.” *Id.* ¶ 13.
7. Each of three offices searched “shared computer drives, Share Point sites, and emails for information about the requested records” because “[t]hese are storage places where DHS employees would typically place information about the products they are working on as well as copies of any final products . . . .” *Id.* ¶ 15.

8. They searched using the search terms “Standard Operating Procedure 303” and “SOP 303.” *Id.*
9. The NPPD initially declined to search, stating that it had no records responsive to the request. *Id.* ¶ 11.
10. DHS sent EPIC a letter stating that it did not locate any responsive records subject to the FOIA. Letter from Mia Day, DHS FOIA Program Specialist, to Amie L. Stepanovich, Assoc. Litigation Counsel, EPIC, Aug. 21, 2012 (attached as Ex. 3).
11. EPIC appealed this determination, arguing that DHS failed to perform an adequate search. EPIC Admin. Appeal, at 2-3, Sept. 13, 2012 (attached as Ex. 4).
12. On appeal, the Office of the Chief Administrative Law Judge for the U.S. Coast Guard, which handles certain FOIA appeals for DHS, concluded that DHS had not sufficiently demonstrated the adequacy of its search. Decision Letter from Joanna Sherry, Attorney Advisor, Office of the Chief ALJ, to Stepanovich, March 25, 2013, at 1 (attached as Ex. 5).
13. The matter was remanded to the agency for further review. *Id.*
14. After this administrative remand, the NPPD conducted a search of its files.  
Holzer Decl. ¶ 19
15. The NPPD located a copy of SOP 303. *Id.*
16. The agency ended its search after concluding that SOP 303 contains all three categories of information sought by EPIC and that no other responsive documents exist. *Id.* ¶¶ 19, 21.

17. The agency determined that the release of names, direct-dial telephone numbers, and email addresses of state homeland security officials contained in SOP 303 would constitute a clearly unwarranted invasion of personal privacy. *Id.* ¶ 23.
18. Accordingly, DHS invokes Exemption 6 to justify this withholding. Holzer *Id.* ¶¶ 22, 23.
19. The agency determined that SOP 303 is a record compiled for law enforcement purposes and that the release of release of the names, telephone numbers, and email addresses of state homeland security officials contained in SOP 303 could reasonably be expected to constitute an unwarranted invasion of personal privacy. *Id.* ¶¶ 20, 24.
20. Accordingly, DHS invokes Exemption 7(C) to justify this withholding. *Id.* ¶¶ 22, 24.
21. The agency determined that SOP 303 is a record compiled for law enforcement purposes and that the release of portions of SOP 303 would disclose the techniques and procedures for law enforcement investigations. *Id.* ¶¶ 20, 25.
22. Accordingly, DHS invokes Exemption 7(E) to justify this withholding. Holzer *Id.* ¶¶ 22, 25.
23. The agency determined that SOP 303 is a record compiled for law enforcement purposes and the release of portions of SOP 303 could reasonably be expected to endanger the life or physical safety of an individual. *Id.* ¶¶ 20, 26.
24. Accordingly, DHS invokes Exemption 7(F) to justify this withholding. Holzer *Id.* ¶¶ 22, 26.

25. The agency determined that portions of SOP 303 are non-exempt, and it is releasing those portions to EPIC. *Id.* ¶ 22.

Dated: June 28, 2013

Respectfully submitted,

STUART F. DELERY  
Acting Assistant Attorney General

RONALD C. MACHEN JR  
United States Attorney

ELIZABETH J. SHAPIRO  
Deputy Director, Federal Programs  
Branch, Civil Division

/s/ Justin M. Sandberg  
JUSTIN M. SANDBERG  
(Ill. Bar No. 6278377)  
Trial Attorney  
U.S. Dept. of Justice, Civil Division,  
Federal Programs Branch  
20 Mass. Ave., NW, Rm. 7302  
Washington, DC 20001  
(202) 514-5838 phone  
(202) 616-8202 fax  
justin.sandberg@usdoj.gov

Attorneys for Defendant

# EXHIBIT 1



**epic.org**

**RECEIVED**

July 10, 2012

**VIA CERTIFIED MAIL**

Mary Ellen Callahan  
Chief Privacy Officer/Chief FOIA Officer  
The Privacy Office  
U.S. Department of Homeland Security  
245 Murray Drive SW, Building 410  
STOP-0655  
Washington, D.C. 20528-0655

JUL 18 2012  
12-0598  
**PRIVACY OFFICE**

1718 Connecticut Ave NW  
Suite 200  
Washington DC 20009  
USA  
+1 202 483 1140 [tel]  
+1 202 483 1248 [fax]  
www.epic.org

Re: Freedom of Information Act Request

To Whom it May Concern:

This letter constitutes a request under the Freedom of Information Act.<sup>1</sup> This request is submitted on behalf of the Electronic Privacy Information Center ("EPIC") to the Department of Homeland Security ("DHS").

**Background**

On March 9, 2006, the National Communications System ("NCS") approved Standard Operating Procedure ("SOP") 303, however it was never released to the public.<sup>2</sup> This secret document codifies a "shutdown and restoration process for use by commercial and private wireless networks during national crisis."<sup>3</sup> In a 2006-2007 Report, the President's National Security Telecommunications Advisory Committee ("NSTAC") indicated that SOP 303 would be implemented under the coordination of the National Coordinating Center ("NCC") of the NSTAC, while the decision to shut down service would be made by state Homeland Security Advisors or individuals at DHS.<sup>4</sup> The report indicates that NCC will determine if a shutdown is necessary based on a "series of questions".<sup>5</sup>

On July 3, 2011, a Bay Area Rapid Transit ("BART") officer in San Francisco shot and killed a homeless man, Charles Hill.<sup>6</sup> The officer alleged later that Hill had

---

<sup>1</sup> 5 U.S.C. § 552 (2011).

<sup>2</sup> National Security Telecommunications Advisory Committee, NSTAC Issue Review 2006-2007 (2007), available at <http://www.ncs.gov/nstac/reports/2007/2006-2007%20NSTAC%20Issue%20Review.pdf>, at 139.

<sup>3</sup> *Id.* at 139.

<sup>4</sup> *Id.* at 139-40.

<sup>5</sup> *Id.* at 139.

<sup>6</sup> *BART Protests: San Francisco Transit Cuts Cellphones to Thwart Demonstrators; First Amendment Debate*, Ned Potter, ABC News, Aug. 16, 2011 <http://abcnews.go.com/Technology/bart-protest-san-francisco-transit-cut-cellphones-prevent/story?id=14311444#.T9jZlvF2m5Y>.

attacked him with a knife and that he had acted in self-defense.<sup>7</sup> The death sparked a major protest against BART on July 11, 2011.<sup>8</sup> Though the protests disrupted service at several transit stations, no one was injured.<sup>9</sup> A second protest was planned one month later, but was cut short after BART officials cut off all cellular service inside four transit stations for a period of three hours.<sup>10</sup> This act prevented any individual on the station platform from sending or receiving phone calls, messages, or other data.<sup>11</sup>

The incident with BART has set off a renewed interest in the government's power to shut down access to the Internet and other communications services.<sup>12</sup> A 2011 Report from the White House asserted that the National Security Council and the Office of Science and Technology Policy have the legal authority to control private communications systems in the United States during times of war or other national emergencies. The Federal Communications Commission plans to implement policies governing the shutdown of communications traffic for the "purpose of ensuring public safety". Also, on July 6, 2012, the White House approved an Executive Order seeking to ensure the continuity of government communications during a national crisis.<sup>13</sup> As part of the Executive Order, DHS was granted the authority to seize private facilities, when necessary, effectively shutting down or limiting civilian communications.<sup>14</sup>

It is impossible to have an informed debate on the need for additional shutdown procedures without public information on the provisions of SOP 303. The complete shutdown of wireless communications for any period of time may be used to prevent the detonation of a bomb through a remote device.<sup>15</sup> However, it can also be leveraged to quell political dissent, prevent protests, and stop the free flow of information and communications. For example, in 2011, the Egyptian government shut down all access to Internet and cellular services for the sole purpose of quieting large-scale anti-government

---

<sup>7</sup> *Id.*

<sup>8</sup> *BART protest causes major delays in service*, Kelly Zito, SFGate, July 11, 2011 <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2011/07/11/BA9G1K9905.DTL>.

<sup>9</sup> *Id.*

<sup>10</sup> Potter, *supra* note 6.

<sup>11</sup> *Id.*

<sup>12</sup> On April 30, 2012, the Federal Communications Commission ("FCC") requested public comment on proposed procedures to guide "intentional interruption of wireless service by government actors for the purpose of ensuring public safety." ([http://transition.fcc.gov/Daily\\_Releases/Daily\\_Business/2012/db0301/DA-12-311A1.pdf](http://transition.fcc.gov/Daily_Releases/Daily_Business/2012/db0301/DA-12-311A1.pdf)). Among other things, the FCC sought feedback on when, if ever, it is appropriate to disrupt wireless services. The comment period closed on May 30, 2012. A final document has not yet been released. However, any final procedures would only apply in circumstances involving public safety, and SOP 303 would remain the governing document for times of national emergency.

<sup>13</sup> White House, Executive Order: Assignment of National Security and Emergency Preparedness Communications Functions (July 6, 2012), *available at* <http://www.whitehouse.gov/the-press-office/2012/07/06/executive-order-assignment-national-security-and-emergency-preparedness->.

<sup>14</sup> *Id.* at Sec. 5.2(e).

<sup>15</sup> *Government asks: when can we shut down wireless service?*, Matthew Lasar, Ars Technica, May 7, 2012 <http://arstechnica.com/tech-policy/2012/05/government-asks-when-can-we-shut-down-wireless-service/>.

protests.<sup>16</sup> Early reports indicated, “The shutdown caused a 90 percent drop in data traffic to and from Egypt, crippling an important communications tool.”<sup>17</sup>

### Documents Requested

In accordance with the facts presented above, EPIC requests the following three (3) categories of records from DHS:

1. The full text of Standard Operating Procedure 303;
2. The full text of the pre-determined “series of questions” that determines if a shutdown is necessary;
3. Any executing protocols or guidelines related to the implementation of Standard Operating Procedure 303, distributed to DHS, other federal agencies, or private companies, including protocols related to oversight of shutdown determinations.

### Request for Expedited Processing

This request warrants expedited processing because it is made by “a person primarily engaged in disseminating information...” and it pertains to a matter about which there is an “urgency to inform the public about an actual or alleged federal government activity.”<sup>18</sup>

EPIC is “primarily engaged in disseminating information.”<sup>19</sup>

There is a particular urgency for the public to obtain information about DHS’ authority to approve the shutdown of wireless networks in the United States. As previously discussed, President Obama signed a new Executive Order on July 6, 2012, which will grant DHS expanded authority to seize control of private communications facilities during times of national crisis.<sup>20</sup> This Executive Order has been the focus of a large number of recent news stories.<sup>21</sup> In addition, numerous cybersecurity bills are currently under consideration, any of which may further extend DHS’ cyber authority.<sup>22</sup>

---

<sup>16</sup> *Egypt Cuts Off Most Internet and Cell Service*, Matt Richtel, New York Times, Jan. 28, 2011, <http://www.nytimes.com/2011/01/29/technology/internet/29cutoff.html>.

<sup>17</sup> *Id.*

<sup>18</sup> 5 U.S.C. § 552(a)(6)(E)(v)(II) (2012); *Al-Fayed v. CIA*, 254 F.3d 300, 306 (D.C. Cir. 2001).

<sup>19</sup> *American Civil Liberties Union v. Department of Justice*, 321 F. Supp. 2d 24, 29 n.5 (D.D.C. 2004).

<sup>20</sup> White House, *supra* note 13.

<sup>21</sup> See, e.g., *White House order on emergency communication rules privacy group*, Jaikumar Vijayan, Computerworld, July 10, 2012 [http://www.computerworld.com/s/article/9228950/White\\_House\\_order\\_on\\_emergency\\_communications\\_rules\\_privacy\\_group](http://www.computerworld.com/s/article/9228950/White_House_order_on_emergency_communications_rules_privacy_group); *White House creates new critical comms management committee*, Mark Rockwell, Gov’t Sec. News, July 9, 2012 <http://www.gsnmagazine.com/node/26716?c=communications>; *CNN Newsroom: Govt. re-prioritizing U.S. communications* (CNN television broadcast July 9, 2012, 2:40 PM), available at <http://newsroom.blogs.cnn.com/2012/07/09/govt-re-prioritizing-u-s-communications/>.

<sup>22</sup> See, e.g., Cybersecurity Act of 2012, S. 2015, 112th Cong. (2012); SECURE IT Act of 2012, H.R. 4263, 112th Cong. (2012).

In order for the public to comment meaningfully on these actions, or subsequent measures, the public must be aware of DHS' current policies and procedures. Neither DHS nor the White House have provided substantive information on the development or implementation of SOP 303. The public must be informed about the government's powers to shut down wireless communications within the United States.

#### Request for "News Media" Fee Status and Fee Waiver

EPIC is a "representative of the news media" for FOIA purposes.<sup>23</sup> Based on our status as a "news media" requester, we are entitled to receive the requested records with only duplication fees assessed.<sup>24</sup> Further, consistent with the Department of Homeland Security regulations, any duplication fees should be waived because disclosure of the records requested herein "is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the Government," and "disclosure of the information 'is not primarily in the commercial interest of [EPIC]'"<sup>25</sup>

This FOIA request involves information on DHS cybersecurity procedures. Responsive documents will hold a great informative value regarding activities of the Department that will have a significant public impact.

EPIC routinely and systematically disseminates information to the public. EPIC maintains several heavily visited websites that highlight breaking news concerning privacy and civil liberties. Two of EPIC's websites, EPIC.org and PRIVACY.org, consistently appear at the top of search engine rankings for searches on "privacy." EPIC also publishes a bi-weekly electronic newsletter, the EPIC Alert, which is distributed to around 20,000 readers, many who report on technology and privacy issues for major news outlets.<sup>26</sup>

In addition, EPIC's FOIA documents have routinely been the subject of national news coverage. On a related matter, EPIC submitted a FOIA request to DHS for documents concerning the Department's surveillance of social networks and news organizations.<sup>27</sup> The documents detailed the Department's implementation of a program to gather information from public social communities on the Internet.<sup>28</sup> EPIC was able to disseminate those documents to the public at large, which resulted in numerous news stories.<sup>29</sup>

<sup>23</sup> *EPIC v. Department of Defense*, 241 F.Supp.2d 5 (D.D.C. 2003).

<sup>24</sup> 6 C.F.R. § 5.11(c)(1)(i) (2011).

<sup>25</sup> *Id.* at (k)(1).

<sup>26</sup> See EPIC: EPIC Alert, <http://epic.org/alert/> (last visited Mar. 14, 2012).

<sup>27</sup> Letter from EPIC to Dept. of Homeland Sec. (Apr. 12, 2011) (on file at <http://epic.org/privacy/socialnet/EPIC-FOIA-DHS-Social-Media-Monitoring-04-12-11.pdf>).

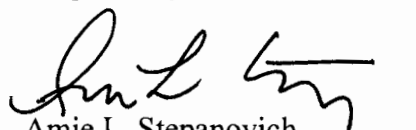
<sup>28</sup> See EPIC: EPIC v. Department of Homeland Security: Media Monitoring, <http://epic.org/foia/epic-v-dhs-media-monitoring/> (last visited July 9, 2012).

<sup>29</sup> See, e.g., *DHS list of words you should never ever blog or tweet. Ever.*, Kevin Fogarty, IT World, May 31, 2012 <http://www.itworld.com/security/279429/dhs-list-words-you-should-never-ever-blog-or-tweet->

EPIC is a non-profit, public interest research center that was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values.<sup>30</sup> EPIC's work is distributed freely through our website and through the bi-weekly EPIC Alert newsletter. EPIC has no clients, no customers, and no shareholders. Therefore, EPIC has no commercial interest that would be furthered by disclosing the requested records.

Thank you for your consideration of this request. As provided in 6 C.F.R. § 5.5(d)(4), I will anticipate your determination on this request for expedited processing within ten (10) business days. For questions regarding this request, I can be contacted at (202)-483-1140 ext. 104 or FOIA@epic.org.

Respectfully Submitted,



Amie L. Stepanovich  
Associate Litigation Counsel  
Electronic Privacy Information Center

John J. Sadlik  
IPIOP Clerk  
Electronic Privacy Information Center

---

ever; *DHS monitoring of social media concerns civil liberties advocates*, Ellen Nakashima, The Washington Post, Jan. 13, 2012 [http://www.washingtonpost.com/world/national-security/dhs-monitoring-of-social-media-worries-civil-liberties-advocates/2012/01/13/gIQANPO7wP\\_story.html](http://www.washingtonpost.com/world/national-security/dhs-monitoring-of-social-media-worries-civil-liberties-advocates/2012/01/13/gIQANPO7wP_story.html); *Federal Contractor Monitored Social Network Sites*, Charlie Savage, New York Times, Jan. 13, 2012 <http://www.nytimes.com/2012/01/14/us/federal-security-program-monitored-public-opinion.html>.

<sup>30</sup> EPIC: About EPIC, <http://epic.org/epic/about.html> (last visited Mar. 20, 2012).

# EXHIBIT 2

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA**

ELECTRONIC PRIVACY INFORMATION  
CENTER,

Plaintiff,

v.

U.S. DEPARTMENT OF HOMELAND  
SECURITY

Defendant.

---

Civil Action No. 13-260 (GK)

**DECLARATION OF JAMES V.M.L. HOLZER, I, IN SUPPORT OF DEFENDANT'S  
MOTION FOR SUMMARY JUDGMENT**

I, James V.M.L. Holzer declare and state as follows:

1. I am the Senior Director of FOIA Operations for the Department of Homeland Security Privacy Office (DHS Privacy). I am the Department official immediately responsible for responding to requests for records under the Freedom of Information Act (FOIA), 5 U.S.C. §552 (the FOIA), the Privacy Act, 5 U.S.C. § 552a (the Privacy Act), and other applicable records access Statutes and Regulations. I have held this position since November 7, 2012. Prior to that, I held the position of Director of Disclosure and FOIA Operations. I have been with the Department since 2009. I make the following statements based upon my personal knowledge, which in turn is based on a personal review of the records in the files established for processing FOIA requests and upon information furnished to me in the course of my official duties. Through the exercise of my official duties, I have also become familiar with the background of this case and have read a copy of the complaint.

2. The purpose of this declaration is to provide an overview of the FOIA process at DHS, and to explain how the FOIA request that is the subject of the instant litigation was processed. This declaration is submitted in support of defendant's motion for summary judgment.

3. The Department of Homeland Security's (DHS) FOIA operations is carried out by the DHS Privacy Office. FOIA requests directed to DHS are reviewed by DHS Privacy, and that office also refers those requests to the DHS offices and components likely to possess responsive documents. DHS Privacy also oversees FOIA and Privacy Act operations throughout DHS.

4. After DHS Privacy receives a FOIA request, that request receives a unique identification number. DHS Privacy uses the unique identification number to track the status of all FOIA requests that it receives. DHS Privacy then reviews the request to determine which DHS office or component is likely to possess responsive documents. This review may include conversations with DHS component FOIA offices to determine if they had received the same request directly from the public and if the component has responsive documents.

5. In addition to DHS Privacy, DHS components maintain offices that handle FOIA requests. These offices also use an automated case tracking systems which assigns case control numbers to all FOIA requests received by that component. Components log all incoming FOIA requests into an automated case tracking system, and input information about each request into the system (including, but not limited to, the requester's name and/or organization and, in the case of FOIA requests, the request's topic). These numbers are used to track the status of incoming FOIA requests.

6. The mission of DHS's National Protection and Programs Directorate (NPPD) is to assure a safe, secure, and resilient infrastructure. There are four subcomponents within NPPD, which are the Federal Protective Service (FPS), Office of Cybersecurity and Communications



(CS&C), Office of Infrastructure Protection (IP), and Office of Biometric Identity Management (OBIM). FPS provides security and law enforcement services to federally owned and leased buildings, facilities, properties. CS&C's mission is to assure the security, resiliency, and reliability of the nation's cyber and communications infrastructure. IP leads a coordinated national effort to reduce risk to our critical infrastructure. OBIM uses innovative technological solutions to provide decision-makers with accurate biometric-based information.

7. NPPD also has a FOIA Office, which processes FOIA requests received directly from the general public by postal delivery or email, and those referred to it by DHS Privacy, DHS component FOIA offices and federal agencies. The NPPD FOIA office processes FOIA requests for all NPPD subcomponents and offices.

8. When the NPPD FOIA office personnel receive a referral or tasking from DHS Privacy or some other source, NPPD FOIA personnel make a determination regarding which NPPD subcomponent or program office may have responsive documents, and then refer the request to the appropriate subcomponent or office.

#### EPIC'S JULY 10, 2012 FOIA REQUEST

9. On July 18, 2012, DHS Privacy received a FOIA request from EPIC dated July 10, 2012. EPIC requested the following categories of records: (1) the full text of Standard Operating Procedure 303 (SOP 303), which describes a shutdown and restoration process for use by "commercial and private wireless networks" in the event of a crisis; (2) the full text of the pre-determined "series of questions" that determines if a shutdown is necessary; and (3) any executing protocols or guidelines related to the implementation of SOP 303, distributed to DHS, other federal agencies, or private companies, including protocols related to oversight of shutdown determinations.

10. When DHS Privacy received EPIC's FOIA request it had to determine which offices at DHS would be most likely to have records responsive to the request. EPIC specifically mentioned the National Communications System (NCS) and the National Coordinating Center for Communications (NCC) in its request, each of which was or is an NPPD organization. The NCS was formerly an organization within NPPD that was established to provide the Federal Government with national security and emergency preparedness communications as well as formulate and implement policies in this area. By Executive Order 13618 on July 6, 2012, the NCS was eliminated, and replaced with an alternate structure for performing the same functions. Also, DHS was directed to establish an organization performing the functions of the NCC. The NCC is a joint government/industry operation, which is housed within the CS&C subcomponent of the NPPD, and which coordinates the initiation, restoration and reconstitution of national security and emergency preparedness communications services nationally. Based on the request's reference to NCS and NCC, DHS Privacy contacted the NPPD FOIA Office to determine if that office was familiar with the subject matter of the request.

11. The NPPD FOIA office believed that there were no responsive records. As discussed more fully below, the NPPD FOIA Office was incorrect, in that NPPD indeed had responsive documents, namely SOP 303. The NPPD FOIA office learned of its mistake later. The mistake was due in part to confusion regarding a similar FOIA request from another requester seeking certain records relating to the activation of SOP 303, but not the SOP itself, as EPIC had requested. Because the two FOIA requests were pending within the same timeframe and dealt with the same general subject matter area, NPPD did not fully appreciate the difference between EPIC's request, which sought only three specific categories of documents (i.e., the full text of SOP 303, the full text of the series of questions used to determine the necessity of shutdown, and

any executing protocols or guidelines), and the other FOIA request, which sought records related to particular security events where the SOP may have been implemented and activated.

12. In addition to referring EPIC's request to NPPD, DHS Privacy also directed the DHS Management Directorate (MGMT), the Office of the Chief Information Officer (OCIO) and the Under Secretary for Management (USM) to search for responsive documents. DHS Privacy believed that these offices would be likely to have documents related to communications policy, such as SOP 303. The DHS Management Directorate is the office responsible for Department budgets and appropriations, expenditure of funds, accounting and finance, procurement, human resources, information technology systems, facilities and equipment, and the identification and tracking of performance measurements. Because of its broad portfolio, MGMT often will know about a policy, procedure or initiative, and DHS Privacy often directs MGMT to search for responsive documents.

13. DHS Privacy directed that OCIO conduct a search because the request related to communications. OCIO is often involved in, and consulted on, information and communication issues, which might have had some information about the subject matter of the request. USM also was tasked to conduct a search because, like MGMT, it has a broad portfolio. The office oversees (i) the promulgation of policy, (ii) operations and (iii) oversight, for each of the critical management lines-of-business. These lines of business include: acquisition, human capital, budget and finance, information technology, capital assets, and security.

14. DHS Privacy sent an acknowledgement to EPIC on July 24, 2012, assigning the matter file number DHS/OS/PRIV 12-0598 and indicated that DHS Privacy had tasked MGMT, OCIO, and USM with a search based on the opinion that those offices would be most likely to have records responsive to the request.

15. Each office conducted a search for documents related to the SOP, using the search terms “Standard Operating Procedure 303” and “SOP 303.” These offices do not have one database to search for records that are responsive to Freedom of Information and/or Privacy Act requests. Consequently, each of the component offices was tasked to search for records. In this instance, for purposes of coordination, search requests were sent to the Chief of Staffs in each of the three Offices mentioned above. In each case, the offices searched shared computer drives, Share Point sites, and emails for information about the requested records. These are the storage places where DHS employees would typically place information about the products they are working on as well as copies of any final products that are proposed for dissemination or are actually disseminated. In each case, the Offices reported no records responsive to the request.

16. DHS Privacy sent its final response to EPIC on August 21, 2012. In the final response, DHS Privacy said that MGMT, OCIO, and USM, had conducted comprehensive searches for records that would be responsive to the request. DHS Privacy also said that these offices were unable to locate or identify any responsive records.

17. On October 2, 2012, DHS Privacy received an appeal from EPIC dated September 13, 2012. DHS Privacy acknowledged the appeal on October 25, 2012. DHS Privacy forwarded the appeal to the United States Coast Guard, Office of the Chief Administrative Law Judge (ALJ), as that office reviews FOIA appeals on behalf of DHS’ Office of the General Counsel.

18. By the letter dated March 25, 2013, the ALJ notified DHS Privacy that it had reviewed the appeal, and it remanded the matter back to DHS Privacy for further review.

19. On April 19, 2013, DHS Privacy reached out to various offices, including MGMT, OCIO, and USM at DHS Headquarters to again inquire as to whether these offices might have responsive documents. DHS Privacy also contacted NPPD again, at which point, the NPPD

FOIA Office realized that there was confusion about the nature of EPIC's request. The NPPD FOIA Office realized that NPPD would have one or possibly more records responsive to the EPIC request. NPPD conducted a search and quickly identified, in the files of the NCC, the only document that is responsive to the request. Specifically, NPPD consulted with the NCC because the NCC is the author of the SOP and implements the SOP. According to the NCC, there are no other documents that contain either the full text of the questions or any executing protocols or guidelines.

20. SOP 303 was drafted by the NCC and approved by CS&C on March 17, 2006. It has been periodically updated so that names and contact information contained therein remains current. The SOP was compiled for a law enforcement purpose, which includes activities related to national security and homeland security. It was inspired by the Letter to the President on Emergency Wireless Protocol and Recommendations, dated March 1, 2006, and generated by the National Security Telecommunications Advisory Committee (NSTAC), an industry-led Presidential advisory committee established by Executive Order 12382. In the aftermath of the 2005 bombings in the London transportation system, the NSTAC perceived the need for a single governmental process to coordinate determinations of if and when cellular shutdown activities should be undertaken in light of the serious impact on access by the public to emergency communications services during these situations and the need to preserve the public trust in the integrity of the communications infrastructure. Consistent with the NSTAC's recommendation, the NCC developed SOP 303 as a unified voluntary process for the orderly shut-down and restoration of wireless services during critical emergencies such as the threat of radio-activated improvised explosive devices. The SOP establishes a procedure by which state homeland

security officials can directly engage with wireless carriers, and it establishes factual authentication procedures for decision-makers.

21. Included as part of SOP 303 itself are the two other categories of records that EPIC seeks, *i.e.*, the full text of the pre-determined series of questions that determines if a shutdown is necessary, and the executing protocols related to the implementation of SOP 303. Again, DHS Privacy, in conjunction with the NCC, determined that the SOP is the only responsive document because there are no other documents that contain the full text of the questions or any executing protocols.

22. Portions of the SOP are being withheld pursuant to FOIA Exemptions b(6), b(7)(c), b(7)(e), and b(7)(f), as the SOP contains security procedures and related information regarding the shutdown of cell phone service during various types of homeland security incidents, and personal information about certain law enforcement officials. After a review for segregability, NPPD FOIA Office determined that some information in the SOP could be released without compromising law enforcement or privacy objectives. DHS Privacy agrees with the assessment.

23. FOIA Exemption b(6) protects from disclosure information about individuals when the disclosure of the information "would constitute a clearly unwarranted invasion of personal privacy." 5 U.S.C. § 552 (b)(6). DHS applied the b(6) exemption to protect the names, direct-dial telephone numbers, and email addresses for state homeland security officials who have an expectation of privacy. The redacted information does not directly shed light on the operations or activities of the government. The release of this information would constitute an unwarranted invasion of personal privacy, possibly subject the persons to harassment by the public and inquiries by the media, and potentially facilitate targeting of these officials by bad actors.

24. FOIA Exemption b(7)(c) permits the withholding of personal information in law

enforcement records. DHS applied the b(7)(c) exemption to protect the names, direct-dial telephone numbers and e-mail addresses of high-ranking officials within each state's homeland security agency. The release of this information would not shed lights on the agency's operations or activities and would constitute an unwarranted invasion of personal privacy, possibly subject the persons to harassment by the public and inquiries by the media, and potentially facilitate targeting of these officials by bad actors.

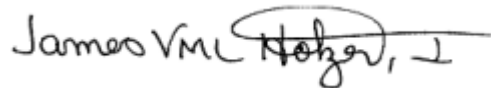
25. FOIA Exemption b(7)(e) permits the withholding of law enforcement information that "would disclose techniques and procedures for law enforcement investigations." The b(7)(e) exemption applies because the requested document contains a homeland security procedure primarily intended to efficiently and effectively deter the triggering of radio-activated improvised explosive devices. During the course of incidents involving the potential for improvised explosive devices to be dispersed over a wide geographic area, orderly deactivation of wireless networks may be the best option for preventing and/or mitigating explosions that would endanger life and property. SOP 303 establishes a protocol for verifying that circumstances exist that would justify shutting down wireless networks. It also ensures that decision makers consider potential public safety hazards when deciding whether to shut-down a wireless network, such as the inability of first-responders and the public to use wireless phones for calls, including 911 calls. In addition, SOP 303 provides a step-by-step process for the orderly shut-down of wireless networks following verification of the facts and appropriate weighing of the circumstances. Finally, SOP 303 coordinates orderly resumption of wireless service. Making SOP 303 public would enable bad actors to circumvent or interfere with a law enforcement strategy designed to prevent activation of improvised explosive devices by providing information about when shutdown procedures are used and how a shutdown is

executed.

26. FOIA Exemption b(7)(F) permits the withholding of records necessary to protect the physical safety of “any individual.” Making SOP 303 public would, *e.g.*, enable bad actors to insert themselves into the process of shutting down or reactivating wireless networks by appropriating verification methods and then impersonating officials designated for involvement in the verification process. The aim of such bad actors would be to disable the protocol so that they could freely use wireless networks to activate the improvised explosive devices. Given that disclosure of the requested information could reasonably lead to circumvention of or interference with a procedure aimed at preventing the triggering of improvised explosive devices, there is a reasonable expectation that disclosure could reasonably endanger individuals’ lives or physical safety.

I declare under penalty of perjury that the foregoing is true and correct.

Executed this 28th day of June, 2013.

A handwritten signature in black ink that reads "James V.M.L. Holzer, J". The signature is written in a cursive, somewhat stylized font. The "J" at the end is a large, sweeping flourish.

---

James V.M.L. Holzer



# EXHIBIT 3



Homeland  
Security

Privacy Office, Mail Stop 0655

August 21, 2012

Amie L. Stepanovich  
Associate Litigation Counsel  
Electronic Privacy Information Center  
1718 Connecticut Avenue, NW  
Suite 200  
Washington, DC 20009

Re: **DHS/OS/PRIV 12-0598**

Dear Ms. Stepanovich:

This is the final response to your Freedom of Information Act (FOIA) request to the Department of Homeland Security (DHS), dated July 10, 2012, and received by this office on July 18, 2012.

You are seeking the following records:

1. The full text of Standard Operating Procedure 303;
2. The full text of the pre-determined "series of questions" that determine if a shutdown is necessary;
3. Any executing protocols or guidelines related to the implementation of Standard Operating Procedure 303, distributed to DHS, other federal agencies, or private companies, including protocols related to oversight of shutdown determinations.

We conducted a comprehensive search of files within the DHS, Management Directorate (MGMT), Office of the Chief Information Officer (CIO) and the Under Secretary for Management (USM), for records that would be responsive to your request. Unfortunately, we were unable to locate or identify any responsive records.

While an adequate search was conducted, you have the right to appeal this determination that no records exist within MGMT-CIO and MGMT-USM that would be responsive to your request. Should you wish to do so, you must send your appeal and a copy of this letter, within 60 days of the date of this letter, to: Associate General Counsel (General Law), U.S. Department of Homeland Security, Washington, D.C. 20528, following the procedures outlined in the DHS FOIA regulations at 6 C.F.R. § 5.9. Your envelope and letter should be marked "FOIA Appeal." Copies of the FOIA and DHS regulations are available at [www.dhs.gov/foia](http://www.dhs.gov/foia).

The Office of Government Information Services (OGIS) also mediates disputes between FOIA requesters and Federal agencies as a non-exclusive alternative to litigation. If you are requesting access to your own records (which is considered a Privacy Act request), you should know that OGIS does not have the authority to handle requests made under the Privacy Act of 1974. If you wish to contact OGIS, you may email them at [ogis@nara.gov](mailto:ogis@nara.gov) or call 1-877-684-6448.

Provisions of the FOIA allow us to recover part of the cost of complying with your request. In this instance, because the cost is below the \$14 minimum, there is no charge.

If you need to contact our office concerning this request, please call 866-431-0486 and refer to **DHS/OS/PRIV 12-0598**.

Sincerely,

A handwritten signature in black ink that reads "Mia Day". The signature is written in a cursive, flowing style.

Mia Day  
FOIA Program Specialist

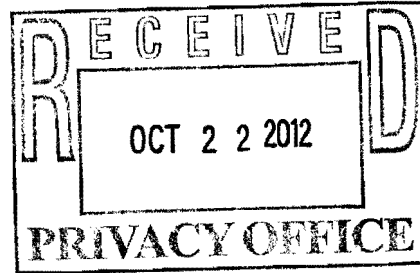
# EXHIBIT 4

**epic.org**

September 13, 2012

**VIA CERTIFIED MAIL**

Associate General Counsel (General Law)  
U.S. Department of Homeland Security  
Washington, D.C. 20528



1718 Connecticut Ave NW  
Suite 200  
Washington DC 20009  
USA  
+1 202 483 1140 [tel]  
+1 202 483 1248 [fax]  
www.epic.org

**Re: Freedom of Information Act Appeal, File No. DHS/OS/PRIV 12-0598**

To Whom it May Concern:

This letter constitutes an appeal under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, and is submitted to the U.S. Department of Homeland Security ("DHS") by the Electronic Privacy Information Center ("EPIC").

On July 10, 2012, EPIC requested, via certified mail, agency records related to Standard Operating Procedure ("SOP") 303. Specifically, EPIC requested the following three (3) categories of records:

1. The full text of Standard Operating Procedure 303;
2. The full text of the pre-determined "series of questions" that determine if a shutdown is necessary;
3. Any executing protocols or guidelines related to the implementation of Standard Operating Procedure 303, distributed to DHS, other federal agencies, or private companies, including protocols related to oversight of shutdown determinations.<sup>1</sup>

In addition, EPIC's FOIA Request stated that EPIC was a news media organization for fee purposes, and requested a waiver of all fees associated with the request. EPIC's FOIA Request also asked for expedited processing on the basis of an "urgency to inform the public about an actual or alleged federal government activity."

DHS acknowledged EPIC's FOIA Request by letter dated July 24, 2012.<sup>2</sup> DHS did not make a determination as to EPIC's request for expedited processing, but invoked a 10-day extension due to the "unusual circumstance" that EPIC's FOIA Request is "of substantial interest" to two or more components of DHS or another agency. DHS conditionally granted EPIC's fee waiver request, indicated that the appropriate

<sup>1</sup> Letter from Amie Stepanovich, Associate Litigation Counsel, EPIC, to Mary Ellen Callahan, Chief Privacy Officer / Chief FOIA Officer, Department of Homeland Security (July 10, 2012) (Appendix 1) [hereinafter *EPIC's FOIA Request*].

<sup>2</sup> Letter from Mia Day, FOIA Program Specialist, DHS to Amie Stepanovich, Associate Litigation Counsel, EPIC (July 24 2012) (Appendix 2).

component had been queried, and assigned EPIC's FOIA Request reference number DHS/OS/PRIV 12-0598.<sup>3</sup>

DHS issued a final response by letter dated August 21, 2012. DHS FBI informed EPIC that the agency was "unable to locate or identify any responsive records."<sup>4</sup> DHS notified EPIC of EPIC's right to appeal the DHS' decision within 60 days.<sup>5</sup>

### EPIC Appeals DHS' Failure to Perform a Sufficient Search for Records

EPIC hereby appeals the sufficiency of the DHS' search regarding EPIC's FOIA Request. Agencies fulfill search obligations if they "can demonstrate beyond material doubt that [their] search was 'reasonably calculated to uncover all relevant documents'."<sup>6</sup> Further, "the adequacy of the search is not determined by its results, but by the method of the search itself."<sup>7</sup>

EPIC's FOIA Request firmly established the identity and existence of SOP 303.<sup>8</sup> A publicly available document explains that SOP 303 was approved by the National Communications System ("NCS"), in 2006.<sup>9</sup> NCS was first formed in 1962, but was transferred to DHS in 2003 and became part of DHS' "Directorate for Preparedness" under the Information Analysis and Infrastructure Sharing and Analysis Center in 2005.<sup>10</sup> Many of the NCS programs are now led by the DHS Office of Cybersecurity and Communications within the National Protection and Programs Directorate.<sup>11</sup>

Despite the detail provided in EPIC's FOIA Request, DHS now asserts that there are no "responsive records". DHS has not adequately demonstrated that they have conducted a search that was "reasonably calculated to uncover all relevant documents." In fact, DHS admits that it only searched files within the Management Directorate ("MGMT") Office of the Chief Information Officer ("CIO") and the Under Secretary for Management ("USM").<sup>12</sup> Notably, DHS did not search the Federal Emergency

<sup>3</sup> *Id.*

<sup>4</sup> Letter from Mia Day, FOIA Program Specialist, DHS to Amie Stepanovich, EPIC (Aug. 21, 2012) (Appendix 3).

<sup>5</sup> *Id.*

<sup>6</sup> *Ancient Coin Collectors Guild v. U.S. Dep't of State*, 641 F.3d 504, 514 (D.C. Cir. 2011) (quoting *Truitt v. Dep't of State*, 897 F.2d 540, 542 (D.C. Cir. 1990)).

<sup>7</sup> *North v. U.S. Dep't of Justice*, 774 F. Supp. 2d 217, 222 (D.D.C. 2011); *Weisberg v. U.S. Dep't of Justice*, 745 F.2d 1476, 1485 (D.C. Cir. 1984).

<sup>8</sup> See *EPIC's FOIA Request*, *supra* note 1 at 1 ("On March 9, 2006, the National Communications System ("NCS") approved Standard Operating Procedure ("SOP") 202, however it was never released to the public." (internal citations omitted)).

<sup>9</sup> National Security Telecommunications Advisory Committee, NSTAC Issue Review 2006-2007 (2007), available at <http://www.ncs.gov/nstac/reports/2007/2006-2007%20NSTAC%20Issue%20Review.pdf>, at 139.

<sup>10</sup> See Background and History of the NCS, National Communications System, <http://www.ncs.gov/about.html> (last visited Sept. 6, 2012). The Directorate of Preparedness was distributed within FEMA Who Joined DHS, Department of Homeland Security, <http://www.dhs.gov/who-joined-dhs> (last visited Sept. 6, 2012).

<sup>11</sup> *Id.*

<sup>12</sup> See Letter from Mia Day, *supra* note 4 at 1.

Management Agency (“FEMA”) or the NPPD, the two components most likely to possess responsive records. DHS’ failure to demonstrate an adequate search, identify all responsive records, and to release all non-exempt documents violates the FOIA.

### EPIC Appeals DHS’ Treatment of EPIC’s FOIA Request

In 2011, EPIC wrote to the Office of Government Information Services (“OGIS”) concerning DHS’ practice of conducting political review of FOIA requests. EPIC noted:

Unfortunately, under a DHS policy in effect since 2006, political appointees have received detailed information about the identity of FOIA requesters and the topics of their requests in weekly reports before FOIA career staff to provide Secretary Napolitano’s political staff with information, including where a requester lives, the requester’s affiliation, and descriptions of the requesting organization’s mission. Despite DHS protestations that the policy has been retracted, there has been no publication about the new policy or the end of the old policy. This policy is contrary to federal law and Supreme Court holdings, as the FOIA does not permit agencies to select FOIA requests for political scrutiny of either the request or the requester.<sup>13</sup>

In a report issued shortly after EPIC’s letter was submitted, the House Committee on Oversight and Government Reform noted, “through the course of an eight-month investigation that political staff under DHS Secretary Janet Napolitano have corrupted the agency’s FOIA compliance procedures, exerted political pressure on FOIA compliance officers, and undermined the federal government’s accountability to the American people.”<sup>14</sup>

DHS’ assertion that EPIC’s FOIA Request “is of substantial interest to two or more components of this Department or of substantial interest to another agency” and that DHS would “have to consult with those entities before we issue a final response” presumes that DHS has returned to its practice of politically vetting FOIA requests. This practice is contrary to the FOIA and should be ceased immediately.<sup>15</sup> DHS should explain why EPIC’s FOIA Request was “of substantial interest,” what “substantial interest” indicates in this context, and what entities were consulted with prior to the issuance of a final determination on the substance of EPIC’s FOIA Request.

<sup>13</sup> Letter from Marc Rotenber, Executive Director, EPIC, et al, to the Honorable Darrell E. Issa, Chairman, House Committee on Oversight and Government Reform and the Honorable Elijah Cummings, Ranking Member, House Committee on Oversight and Government Reform (Feb. 15, 2011), *available at* [http://epic.org/open\\_gov/foia/Issa\\_FOIA\\_Oversight\\_Ltr\\_02\\_15\\_11.pdf](http://epic.org/open_gov/foia/Issa_FOIA_Oversight_Ltr_02_15_11.pdf).

<sup>14</sup> A New Era of Openness? How and Why Political Staff at DHS Interfered with the FOIA Process 3 (U.S. House of Representatives 2011), *available at* [http://oversight.house.gov/wp-content/uploads/2012/02/DHS\\_REPORT\\_FINAL\\_FINAL\\_4\\_01\\_11.pdf](http://oversight.house.gov/wp-content/uploads/2012/02/DHS_REPORT_FINAL_FINAL_4_01_11.pdf).

<sup>15</sup> See 5 U.S.C. § 552(a)(6)(A)-(B) (setting out statutorily mandated deadlines for the processing of FOIA requests).

EPIC Renews Its Request for “News Media” Fee Status

At this time, EPIC reiterates all arguments that it should be granted “news media” fee status. EPIC is a non-profit, educational organization that routinely and systematically disseminates information to the public. EPIC is a representative of the news media.<sup>16</sup>

EPIC’s status as a “news media” requester entitles it to receive requested records with only duplication fees assessed. In addition, because disclosure of this information will “contribute significantly to the public understanding of the operations or activities of the government,” any duplication fees should be waived.

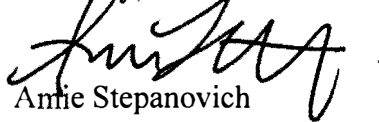
EPIC Renews Its Request for Expedited Treatment and Requests Expedited Treatment of this Appeal

For all of the reasons set forth therein, EPIC’s FOIA Request warrants expedited processing. In addition, EPIC requests expedited processing on this Appeal for each of the reasons set forth above.

Conclusion

EPIC appeals the DHS’ failure to conduct an adequate search in response to EPIC’s FOIA Request. Thank you for your prompt response to this appeal. I anticipate that you will produce responsive documents within 10 working days of this appeal. If you have any questions, please contact me at (202) 483-1140 x 104 or foia@epic.org.

Sincerely,



Annie Stepanovich  
Associate Litigation Counsel  
Electronic Privacy Information Center

/enclosures

---

<sup>16</sup> *EPIC v. Dep’t of Defense*, 241 F. Supp. 2d. 5 (D.D.C. 2003).



**Appendix 1**

EPIC's July 10, 2012 FOIA Request to DHS

# epic.org

July 10, 2012

**VIA CERTIFIED MAIL**

Mary Ellen Callahan  
Chief Privacy Officer/Chief FOIA Officer  
The Privacy Office  
U.S. Department of Homeland Security  
245 Murray Drive SW, Building 410  
STOP-0655  
Washington, D.C. 20528-0655

1718 Connecticut Ave NW  
Suite 200  
Washington DC 20009  
USA  
+1 202 483 1140 [tel]  
+1 202 483 1248 [fax]  
www.epic.org

Re: Freedom of Information Act Request

To Whom it May Concern:

This letter constitutes a request under the Freedom of Information Act.<sup>1</sup> This request is submitted on behalf of the Electronic Privacy Information Center ("EPIC") to the Department of Homeland Security ("DHS").

**Background**

On March 9, 2006, the National Communications System ("NCS") approved Standard Operating Procedure ("SOP") 303, however it was never released to the public.<sup>2</sup> This secret document codifies a "shutdown and restoration process for use by commercial and private wireless networks during national crisis."<sup>3</sup> In a 2006-2007 Report, the President's National Security Telecommunications Advisory Committee ("NSTAC") indicated that SOP 303 would be implemented under the coordination of the National Coordinating Center ("NCC") of the NSTAC, while the decision to shut down service would be made by state Homeland Security Advisors or individuals at DHS.<sup>4</sup> The report indicates that NCC will determine if a shutdown is necessary based on a "series of questions".<sup>5</sup>

On July 3, 2011, a Bay Area Rapid Transit ("BART") officer in San Francisco shot and killed a homeless man, Charles Hill.<sup>6</sup> The officer alleged later that Hill had

---

<sup>1</sup> 5 U.S.C. § 552 (2011).

<sup>2</sup> National Security Telecommunications Advisory Committee, NSTAC Issue Review 2006-2007 (2007), available at <http://www.ncs.gov/nstac/reports/2007/2006-2007%20NSTAC%20Issue%20Review.pdf>, at 139.

<sup>3</sup> *Id.* at 139.

<sup>4</sup> *Id.* at 139-40.

<sup>5</sup> *Id.* at 139.

<sup>6</sup> *BART Protests: San Francisco Transit Cuts Cellphones to Thwart Demonstrators; First Amendment Debate*, Ned Potter, ABC News, Aug. 16, 2011 <http://abcnews.go.com/Technology/bart-protest-san-francisco-transit-cut-cellphones-prevent/story?id=14311444#.T9jZlvF2m5Y>.

attacked him with a knife and that he had acted in self-defense.<sup>7</sup> The death sparked a major protest against BART on July 11, 2011.<sup>8</sup> Though the protests disrupted service at several transit stations, no one was injured.<sup>9</sup> A second protest was planned one month later, but was cut short after BART officials cut off all cellular service inside four transit stations for a period of three hours.<sup>10</sup> This act prevented any individual on the station platform from sending or receiving phone calls, messages, or other data.<sup>11</sup>

The incident with BART has set off a renewed interest in the government's power to shut down access to the Internet and other communications services.<sup>12</sup> A 2011 Report from the White House asserted that the National Security Council and the Office of Science and Technology Policy have the legal authority to control private communications systems in the United States during times of war or other national emergencies. The Federal Communications Commission plans to implement policies governing the shutdown of communications traffic for the "purpose of ensuring public safety". Also, on July 6, 2012, the White House approved an Executive Order seeking to ensure the continuity of government communications during a national crisis.<sup>13</sup> As part of the Executive Order, DHS was granted the authority to seize private facilities, when necessary, effectively shutting down or limiting civilian communications.<sup>14</sup>

It is impossible to have an informed debate on the need for additional shutdown procedures without public information on the provisions of SOP 303. The complete shutdown of wireless communications for any period of time may be used to prevent the detonation of a bomb through a remote device.<sup>15</sup> However, it can also be leveraged to quell political dissent, prevent protests, and stop the free flow of information and communications. For example, in 2011, the Egyptian government shut down all access to Internet and cellular services for the sole purpose of quieting large-scale anti-government

---

<sup>7</sup> *Id.*

<sup>8</sup> *BART protest causes major delays in service*, Kelly Zito, SFGate, July 11, 2011 <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2011/07/11/BA9G1K9905.DTL>.

<sup>9</sup> *Id.*

<sup>10</sup> Potter, *supra* note 6.

<sup>11</sup> *Id.*

<sup>12</sup> On April 30, 2012, the Federal Communications Commission ("FCC") requested public comment on proposed procedures to guide "intentional interruption of wireless service by government actors for the purpose of ensuring public safety." ([http://transition.fcc.gov/Daily\\_Releases/Daily\\_Business/2012/db0301/DA-12-311A1.pdf](http://transition.fcc.gov/Daily_Releases/Daily_Business/2012/db0301/DA-12-311A1.pdf)). Among other things, the FCC sought feedback on when, if ever, it is appropriate to disrupt wireless services. The comment period closed on May 30, 2012. A final document has not yet been released. However, any final procedures would only apply in circumstances involving public safety, and SOP 303 would remain the governing document for times of national emergency.

<sup>13</sup> White House, Executive Order: Assignment of National Security and Emergency Preparedness Communications Functions (July 6, 2012), *available at* <http://www.whitehouse.gov/the-press-office/2012/07/06/executive-order-assignment-national-security-and-emergency-preparedness->.

<sup>14</sup> *Id.* at Sec. 5.2(e).

<sup>15</sup> *Government asks: when can we shut down wireless service?*, Matthew Lasar, Ars Technica, May 7, 2012 <http://arstechnica.com/tech-policy/2012/05/government-asks-when-can-we-shut-down-wireless-service/>.

protests.<sup>16</sup> Early reports indicated, “The shutdown caused a 90 percent drop in data traffic to and from Egypt, crippling an important communications tool.”<sup>17</sup>

### Documents Requested

In accordance with the facts presented above, EPIC requests the following three (3) categories of records from DHS:

1. The full text of Standard Operating Procedure 303;
2. The full text of the pre-determined “series of questions” that determines if a shutdown is necessary;
3. Any executing protocols or guidelines related to the implementation of Standard Operating Procedure 303, distributed to DHS, other federal agencies, or private companies, including protocols related to oversight of shutdown determinations.

### Request for Expedited Processing

This request warrants expedited processing because it is made by “a person primarily engaged in disseminating information...” and it pertains to a matter about which there is an “urgency to inform the public about an actual or alleged federal government activity.”<sup>18</sup>

EPIC is “primarily engaged in disseminating information.”<sup>19</sup>

There is a particular urgency for the public to obtain information about DHS’ authority to approve the shutdown of wireless networks in the United States. As previously discussed, President Obama signed a new Executive Order on July 6, 2012, which will grant DHS expanded authority to seize control of private communications facilities during times of national crisis.<sup>20</sup> This Executive Order has been the focus of a large number of recent news stories.<sup>21</sup> In addition, numerous cybersecurity bills are currently under consideration, any of which may further extend DHS’ cyber authority.<sup>22</sup>

---

<sup>16</sup> *Egypt Cuts Off Most Internet and Cell Service*, Matt Richtel, New York Times, Jan. 28, 2011, <http://www.nytimes.com/2011/01/29/technology/internet/29cutoff.html>.

<sup>17</sup> *Id.*

<sup>18</sup> 5 U.S.C. § 552(a)(6)(E)(v)(II) (2012); *Al-Fayed v. CIA*, 254 F.3d 300, 306 (D.C. Cir. 2001).

<sup>19</sup> *American Civil Liberties Union v. Department of Justice*, 321 F. Supp. 2d 24, 29 n.5 (D.D.C. 2004).

<sup>20</sup> White House, *supra* note 13.

<sup>21</sup> See, e.g., *White House order on emergency communication rules privacy group*, Jaikumar Vijayan, Computerworld, July 10, 2012

[http://www.computerworld.com/s/article/9228950/White\\_House\\_order\\_on\\_emergency\\_communications\\_rules\\_privacy\\_group](http://www.computerworld.com/s/article/9228950/White_House_order_on_emergency_communications_rules_privacy_group); *White House creates new critical comms management committee*, Mark Rockwell, Gov’t Sec. News, July 9, 2012 <http://www.gsnmagazine.com/node/26716?c=communications>; *CNN Newsroom: Govt. re-prioritizing U.S. communications* (CNN television broadcast July 9, 2012, 2:40 PM), available at <http://newsroom.blogs.cnn.com/2012/07/09/govt-re-prioritizing-u-s-communications/>.

<sup>22</sup> See, e.g., Cybersecurity Act of 2012, S. 2015, 112th Cong. (2012); SECURE IT Act of 2012, H.R. 4263, 112th Cong. (2012).

In order for the public to comment meaningfully on these actions, or subsequent measures, the public must be aware of DHS' current policies and procedures. Neither DHS nor the White House have provided substantive information on the development or implementation of SOP 303. The public must be informed about the government's powers to shut down wireless communications within the United States.

#### Request for "News Media" Fee Status and Fee Waiver

EPIC is a "representative of the news media" for FOIA purposes.<sup>23</sup> Based on our status as a "news media" requester, we are entitled to receive the requested records with only duplication fees assessed.<sup>24</sup> Further, consistent with the Department of Homeland Security regulations, any duplication fees should be waived because disclosure of the records requested herein "is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the Government," and "disclosure of the information 'is not primarily in the commercial interest of [EPIC]'"<sup>25</sup>.

This FOIA request involves information on DHS cybersecurity procedures. Responsive documents will hold a great informative value regarding activities of the Department that will have a significant public impact.

EPIC routinely and systematically disseminates information to the public. EPIC maintains several heavily visited websites that highlight breaking news concerning privacy and civil liberties. Two of EPIC's websites, EPIC.org and PRIVACY.org, consistently appear at the top of search engine rankings for searches on "privacy." EPIC also publishes a bi-weekly electronic newsletter, the EPIC Alert, which is distributed to around 20,000 readers, many who report on technology and privacy issues for major news outlets.<sup>26</sup>

In addition, EPIC's FOIA documents have routinely been the subject of national news coverage. On a related matter, EPIC submitted a FOIA request to DHS for documents concerning the Department's surveillance of social networks and news organizations.<sup>27</sup> The documents detailed the Department's implementation of a program to gather information from public social communities on the Internet.<sup>28</sup> EPIC was able to disseminate those documents to the public at large, which resulted in numerous news stories.<sup>29</sup>

<sup>23</sup> *EPIC v. Department of Defense*, 241 F.Supp.2d 5 (D.D.C. 2003).

<sup>24</sup> 6 C.F.R. § 5.11(c)(1)(i) (2011).

<sup>25</sup> *Id.* at (k)(1).

<sup>26</sup> See EPIC: EPIC Alert, <http://epic.org/alert/> (last visited Mar. 14, 2012).

<sup>27</sup> Letter from EPIC to Dept. of Homeland Sec. (Apr. 12, 2011) (on file at <http://epic.org/privacy/socialnet/EPIC-FOIA-DHS-Social-Media-Monitoring-04-12-11.pdf>).

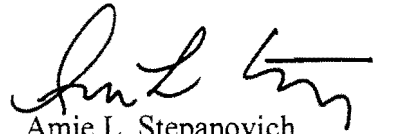
<sup>28</sup> See EPIC: EPIC v. Department of Homeland Security: Media Monitoring, <http://epic.org/foia/epic-v-dhs-media-monitoring/> (last visited July 9, 2012).

<sup>29</sup> See, e.g., *DHS list of words you should never ever blog or tweet*, Ever., Kevin Fogarty, IT World, May 31, 2012 <http://www.itworld.com/security/279429/dhs-list-words-you-should-never-ever-blog-or-tweet->

EPIC is a non-profit, public interest research center that was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values.<sup>30</sup> EPIC's work is distributed freely through our website and through the bi-weekly EPIC Alert newsletter. EPIC has no clients, no customers, and no shareholders. Therefore, EPIC has no commercial interest that would be furthered by disclosing the requested records.

Thank you for your consideration of this request. As provided in 6 C.F.R. § 5.5(d)(4), I will anticipate your determination on this request for expedited processing within ten (10) business days. For questions regarding this request, I can be contacted at (202)-483-1140 ext. 104 or FOIA@epic.org.

Respectfully Submitted,

A handwritten signature in black ink, appearing to read 'Amie L. Stepanovich', followed by a period.

Amie L. Stepanovich  
Associate Litigation Counsel  
Electronic Privacy Information Center

John J. Sadlik  
IPIOP Clerk  
Electronic Privacy Information Center

---

ever; *DHS monitoring of social media concerns civil liberties advocates*, Ellen Nakashima, The Washington Post, Jan. 13, 2012 [http://www.washingtonpost.com/world/national-security/dhs-monitoring-of-social-media-worries-civil-liberties-advocates/2012/01/13/gIqANPO7wP\\_story.html](http://www.washingtonpost.com/world/national-security/dhs-monitoring-of-social-media-worries-civil-liberties-advocates/2012/01/13/gIqANPO7wP_story.html); *Federal Contractor Monitored Social Network Sites*, Charlie Savage, New York Times, Jan. 13, 2012 <http://www.nytimes.com/2012/01/14/us/federal-security-program-monitored-public-opinion.html>.

<sup>30</sup> EPIC: About EPIC, <http://epic.org/epic/about.html> (last visited Mar. 20, 2012).

**Appendix 2**

DHS' July 24, 2012 Acknowledgement of EPIC's FOIA Request

U.S. Department of Homeland Security  
Washington, DC 20528-0655



**Homeland  
Security**

Privacy Office, Mail Stop 0655

July 24, 2012

Amie L. Stepanovich  
Associate Litigation Counsel  
Electronic Privacy Information Center  
1718 Connecticut Avenue, NW  
Suite 200  
Washington, DC 20009

Re: **DHS/OS/PRIV 12-0598**

Dear Ms. Stepanovich:

This acknowledges receipt of your July 10, 2012, Freedom of Information Act (FOIA) request to the Department of Homeland Security (DHS), for the following records:

1. The full text of Standard Operating Procedure 303;
2. The full text of the pre-determined "series of questions" that determine if a shutdown is necessary;
3. Any executing protocols or guidelines related to the implementation of Standard Operating Procedure 303, distributed to DHS, other federal agencies, or private companies, including protocols related to oversight of shutdown determinations.

Your request was received in this office on July 18, 2012.

Per Section 5.5(a) of the DHS FOIA regulations, 6 C.F.R. Part 5, the Department processes FOIA requests according to their order of receipt. Although DHS' goal is to respond within 20 business days of receipt of your request, the FOIA does permit a 10-day extension of this time period. As the subject matter of your request is of substantial interest to two or more components of this Department or of substantial interest to another agency, we will need to consult with those entities before we issue a final response. Due to these unusual circumstances, DHS will invoke a 10-day extension for your request, as allowed by Title 5 U.S.C. § 552(a)(6)(B). If you care to narrow the scope of your request, please contact our office. We will make every effort to comply with your request in a timely manner.

You have requested a fee waiver. The DHS FOIA Regulations at 6 CFR § 5.11(k)(2), set forth six factors DHS is required to evaluate in determining whether the applicable legal standard for a



fee waiver has been met: (1) Whether the subject of the requested records concerns “the operations or activities of the government;” (2) Whether the disclosure is “likely to contribute” to an understanding of government operations or activities; (3) Whether disclosure of the requested information will contribute to the understanding of the public at large, as opposed to the individual understanding of the requestor or a narrow segment of interested persons; (4) Whether the contribution to public understanding of government operations or activities will be “significant;” (5) Whether the requestor has a commercial interest that would be furthered by the requested disclosure; and (6) Whether the magnitude of any identified commercial interest to the requestor is sufficiently large in comparison with the public interest in disclosure, that disclosure is primarily in the commercial interest of the requestor.

Upon review of the subject matter of your request, and an evaluation of the six factors identified above, DHS has determined that it will conditionally grant your request for a fee waiver. The fee waiver determination will be based upon a sampling of the responsive documents received from the various DHS program offices as a result of the searches conducted in response to your FOIA request. DHS will, pursuant to DHS regulations applicable to media requestors, process the first 100 pages at no charge. If upon review of these documents, DHS determines that the disclosure of the information contained in those documents does not meet the factors permitting DHS to waive the fees then DHS will at that time either deny your request for a fee waiver entirely or allow for a percentage reduction in the amount of the fees corresponding to the amount of relevant material found that meets the factors allowing for a fee waiver. In either case, DHS will promptly notify you of its final decision regarding your request for a fee waiver and provide you with the responsive records as required by DHS regulations.

In the event that your fee waiver is denied and you determine that you still want the records, provisions of the Act allow us to recover part of the cost of complying with your request. We shall charge you for records in accordance with the DHS Interim FOIA regulations as they apply to media requestors. As a media requester you will be charged 10-cents a page for duplication, although the first 100 pages are free. In the event that your fee waiver is denied, you have agreed to pay up to \$25.00. You will be contacted before any further fees are accrued.

We have queried the appropriate component of DHS for responsive records. If any responsive records are located, they will be reviewed for determination of releasability. Please be assured that one of the processors in our office will respond to your request as expeditiously as possible. We appreciate your patience as we proceed with your request.

Your request has been assigned reference number **DHS/OS/PRIV 12-0598**. Please refer to this identifier in any future correspondence. You may contact this office at 866-431-0486 or at 703-235-0790.

Sincerely,

A handwritten signature in black ink that reads "Mia Day". The signature is written in a cursive, flowing style.

Mia Day  
FOIA Program Specialist

**3**

DHS' August 21, 2012 Final Determination on EPIC's FOIA Request

U.S. Department of Homeland Security  
Washington, DC 20528-0655



**Homeland  
Security**

Privacy Office, Mail Stop 0655

August 21, 2012

Amie L. Stepanovich  
Associate Litigation Counsel  
Electronic Privacy Information Center  
1718 Connecticut Avenue, NW  
Suite 200  
Washington, DC 20009

Re: **DHS/OS/PRIV 12-0598**

Dear Ms. Stepanovich:

This is the final response to your Freedom of Information Act (FOIA) request to the Department of Homeland Security (DHS), dated July 10, 2012, and received by this office on July 18, 2012.

You are seeking the following records:

1. The full text of Standard Operating Procedure 303;
2. The full text of the pre-determined "series of questions" that determine if a shutdown is necessary;
3. Any executing protocols or guidelines related to the implementation of Standard Operating Procedure 303, distributed to DHS, other federal agencies, or private companies, including protocols related to oversight of shutdown determinations.

We conducted a comprehensive search of files within the DHS, Management Directorate (MGMT), Office of the Chief Information Officer (CIO) and the Under Secretary for Management (USM), for records that would be responsive to your request. Unfortunately, we were unable to locate or identify any responsive records.

While an adequate search was conducted, you have the right to appeal this determination that no records exist within MGMT-CIO and MGMT-USM that would be responsive to your request. Should you wish to do so, you must send your appeal and a copy of this letter, within 60 days of the date of this letter, to: Associate General Counsel (General Law), U.S. Department of Homeland Security, Washington, D.C. 20528, following the procedures outlined in the DHS FOIA regulations at 6 C.F.R. § 5.9. Your envelope and letter should be marked "FOIA Appeal." Copies of the FOIA and DHS regulations are available at [www.dhs.gov/foia](http://www.dhs.gov/foia).

The Office of Government Information Services (OGIS) also mediates disputes between FOIA requesters and Federal agencies as a non-exclusive alternative to litigation. If you are requesting access to your own records (which is considered a Privacy Act request), you should know that OGIS does not have the authority to handle requests made under the Privacy Act of 1974. If you wish to contact OGIS, you may email them at [ogis@nara.gov](mailto:ogis@nara.gov) or call 1-877-684-6448.

Provisions of the FOIA allow us to recover part of the cost of complying with your request. In this instance, because the cost is below the \$14 minimum, there is no charge.

If you need to contact our office concerning this request, please call 866-431-0486 and refer to **DHS/OS/PRIV 12-0598**.

Sincerely,

A handwritten signature in black ink that reads "Mia Day". The signature is written in a cursive, flowing style.

Mia Day  
FOIA Program Specialist

**CERTIFIED MAIL™**



7010 2780 0001 9823 5702

ELECTRONIC PRIVACY INFORMATION CENTER

**epic.org**

1718 Connecticut Ave NW  
Suite 200  
Washington DC 20009  
USA

Associate General Counsel  
(General Law)  
U.S. Department of Homeland  
Security  
Washington, D.C. 20528

FOIA Appeal DHS/OS/PRIV 12-  
0598

**1-1**

**1-**

485  
Delivery Point  
Bldg 1

associate general counsel

Processed By: DSS-990M-019  
9/19/2012 11:18:01 AM

70102780000198235702

# EXHIBIT 5

U.S. Department of  
Homeland Security

United States  
Coast Guard



Office of the Administrative Law Judge  
United States Coast Guard

2100 2nd Street S.W., Stop 7000  
Washington, DC 20593  
Staff Symbol: CG-00J  
Phone: 202-372-4446  
Fax: 202-372-4964  
Email: Joanna.M.Sherry@uscg.mil

5720  
March 25, 2013

Amie L. Stepanovich  
Associate Litigation Counsel  
Electronic Privacy Information Center  
1718 Connecticut Avenue, NW  
Suite 200  
Washington, DC 20009

RE: DHS FOIA APPEAL 2013-HQAP-00004

Dear Ms. Stepanovich:

This letter is in response to your letter dated September 13, 2012, appealing the Privacy Office's response to your July 10, 2012 FOIA request. Specifically, you alleged the Agency failed to conduct an adequate search for the full text of Standard Operating Procedure 303; the full text of the pre-determined "series of questions" that determine if a shutdown is necessary; and any executing protocols or guidelines related to the implementation of Standard Operating Procedure 303, distributed to DHS, other federal agencies, or private companies, including protocols related to oversight of shutdown determinations.

Pursuant to a memorandum of agreement, the United States Coast Guard Office of the Chief Administrative Law Judge is reviewing the FOIA appeals for the Department of Homeland Security General Counsel's office. Therefore, the Office of the Chief Administrative Law Judge will be rendering the official appeal decision on behalf of the Department of Homeland Security.

After a thorough review of your appeal and all applicable documents, the Agency's August 21, 2012 decision is being remanded. In the instant case, the record fails to demonstrate that the Privacy Office conducted an adequate search for responsive records within the Management Directorate (MGMT), Office of the Chief Information Officer (CIO), and the Under Secretary for Management (USM). Accordingly, the file is being remanded for further review.

Sincerely,

A handwritten signature in black ink, appearing to read "Joanna Sherry".

Joanna Sherry  
Attorney Advisor  
Office of the Chief Administrative Law Judge  
United States Coast Guard

Copy : James V.M.L. Holzer, I, CIPP/G, FOIA Officer  
Sent: Via first class mail to the above address.

U.S. Department of  
Homeland Security

United States  
Coast Guard



Office of the Administrative Law Judge  
United States Coast Guard

2100 Second Street, S.W.  
Stop 7000  
Washington, DC 20593-7000  
Staff Symbol: CG-00J  
Phone: (202) 372-4446  
Fax: (202) 372-4964  
Email: Joanna.M.Sherry@uscg.mil

5720  
March 25, 2013

## MEMORANDUM

From: Joanna M. Sherry   
Attorney Advisor

Reply to CG-00J  
Attn of: Joanna M. Sherry  
202-372-4440

To: James V.M.L. Holzer, I, MHR, CIPP/G  
Department of Homeland Security  
Privacy Office

Subj: DHS FOIA APPEAL 2013-HQAP-00004

1. This FOIA request is being remanded to your office for further review. The above-captioned FOIA request was filed on or about July 10, 2012 and appealed on July 20, 2012. Based on the record, it is unclear as to whether the Privacy Office performed an adequate search for responsive records.

2. If you have any questions feel free to contact me directly at 202-372-4446.

Enclosure: Remand Letter



# EXHIBIT 6

***EPIC v. DHS*, Civil Action No. 12-260**

***Vaughn* Index**

Document:	1
Page Range:	1 – 30 (Production PDF)
Document description:	NCC STANDARD OPERATING PROCEDURE (SOP) 303

**Exemptions protecting information from release:** (b)(6), (b)(7)(c), (b)(7)(e), (b)(7)(f)

Defendant.

Case No. 1:13-CV-260 (JEB)

**JAMES E. BOASBERG**  
United States District Judge