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. 13-00260 (JEB)

PLAINTIFF'S OPPOSITION TO DEFENDANT'S MOTION FOR SUMMARY JUDGMENT AND CROSS-MOTION FOR SUMMARY JUDGMENT

Plaintiff Electronic Privacy Information Center hereby opposes Defendant U.S. Department of Homeland Security's motion for summary judgment, and cross-moves for summary judgment pursuant to Federal Rule of Civil Procedure 56(a). EPIC respectfully refers the Court to the accompanying memorandum in support of this cross-motion.

Dated: July 26, 2013

Respectfully submitted,

MARC ROTENBERG
President and Executive Director

/s/ Ginger P. McCall
GINGER P. MCCALL
(DC Bar No. 1001104)

DAVID JACOBS*
JULIA HORWITZ**
Electronic Privacy

* Admitted to practice in New York, admission pending in D.C.
** Admitted to practice in Maryland, admission pending in D.C.

Information Center
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009
Telephone: (202) 483-1140
Fax: (202) 483-1248
mccall@epic.org

Attorneys for Plaintiff

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. 13-00260 (JEB)

MEMORANDUM IN SUPPORT OF PLAINTIFF'S OPPOSITION TO DEFENDANT'S MOTION FOR SUMMARY JUDGMENT AND CROSS-MOTION FOR SUMMARY JUDGMENT

INTRODUCTION

This case involves a Freedom of Information Act ("FOIA") request filed by the Electronic Privacy Information Center ("EPIC") for a document known as "Standard Operating Procedure 303" ("SOP 303"). SOP 303 describes a process for the government's deactivation of wireless communications networks in a specific area or an entire metropolitan region. Because the ability to shut down an entire communications network threatens both freedom of speech and public safety, EPIC sought release of SOP 303 to facilitate public awareness and discussion.

The Department of Homeland Security ("DHS") claims that it cannot release SOP 303 because doing so would reveal techniques or procedures for law enforcement investigations or prosecutions. But DHS has demonstrated no connection between the text of SOP 303 and any conceivable investigation or prosecution. DHS also claims that releasing SOP 303 could endanger the lives or physical safety of individuals. However, the speculative risk to unidentified

persons near a nonexistent bomb at an indeterminate date is far too attenuated to justify withholding SOP 303. Thus, the Court should deny DHS's motion and grant EPIC's cross-motion. At a minimum, the Court should ensure that the agency disclose any segregable information that is subject to disclosure under the Act.

FACTUAL AND PROCEDURAL BACKGROUND

On July 10, 2012, EPIC submitted a FOIA request to DHS for information regarding Standard Operating Procedure 303 ("SOP 303"). *See* EPIC FOIA Request, Dkt. 10-1. SOP 303 codifies a "shutdown and restoration process for use by commercial and private wireless networks during national crisis." *Id.* at 2. EPIC noted that the government's deactivation of entire communication networks raised serious First Amendment and public safety concerns, and said that it was "impossible to have an informed debate on the need for additional shutdown procedures without public information on the provisions of SOP 303." *Id.* at 3. To that end, EPIC requested three specific 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.

Id. at 4.

DHS acknowledged the request on July 24, 2012, conditionally granting a fee waiver and assigning the request Reference Number DHS/OS/PRIV 12-0598. DHS Request Acknowledgement, Dkt. 10-4, at 13-14. DHS then granted itself 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. *Id.* at 13.

On August 21, 2012, DHS provided its final response, claiming that the agency was "unable to locate or identify any responsive records." DHS Determination, Dkt. 10-3, at 2. EPIC appealed the adequacy of DHS's search on September 13, 2012, setting forth in detail the evidence for the existence of SOP 303 and for its location within one or more DHS subcomponents. EPIC FOIA Appeal, Dkt. 10-4, at 2. DHS acknowledged EPIC's appeal on October 25, 2012, but failed to make a determination with respect to EPIC's appeal within twenty days, as required by the FOIA. DHS Appeal Acknowledgement (attached as Ex. 1).

On February 27, 2013, EPIC filed EPIC filed this lawsuit under the FOIA, 5 U.S.C. § 552. *See* Compl., Dkt. 1. After filing the complaint, EPIC received a letter from the United States Coast Guard Office of the Chief Administrative Law Judge. Administrative Decision Letter, Dkt. 10-5. The letter indicated that "the record fails to demonstrate that the Privacy Office conducted an adequate search for responsive records" and stated that the filed would be remanded for further review. *Id.* at 2.

On June 28, 2013, DHS filed its motion for summary judgment and provided a copy of SOP 303 to EPIC. With the exception of a few subject headings, the document was entirely redacted. The agency cited FOIA exemptions 6, 7(C), 7(E), and 7(F).[1] *See* SOP 303 (attached as Ex. 2). EPIC now opposes the government's motion for summary judgment and cross-moves for summary judgment.

STANDARD OF REVIEW

The U.S. Supreme Court "repeatedly has stressed the fundamental principle of public access to Government documents that animates the FOIA." *John Doe Agency v. John Doe Corp.*, 493 U.S. 146, 151-52 (1989). As the Court has previously explained, "[t]he basic purpose of

[1] EPIC is not challenging the assertion of Exemptions 6 and 7(C).

FOIA is to ensure an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed." *NLRB v. Robbins Tire & Rubber Co.*, 437 U.S. 214, 242 (1978); *see also Nat'l Archives & Records Admin. v. Favish*, 541 U.S. 157, 171-72 (2004) (knowledge of "what the Government is up to" is "a structural necessity in a real democracy") (internal quotation omitted). "In enacting FOIA, Congress struck the balance it thought right—generally favoring disclosure, subject only to a handful of specified exemptions—and did so across the length and breadth of the Federal Government." *Milner v. Dep't of the Navy*, 131 S. Ct. 1259, 1266 (2011). The FOIA's "basic purpose reflect[s] a general philosophy of full agency disclosure unless information is exempted under clearly delineated statutory language." *U.S. Dep't of Air Force v. Rose*, 425 U.S. 352, 360-61 (1976), quoting S. Rep. No. 89-813, at 3 (1965). FOIA was meant to be a "disclosure statute," not a "withholding statute." *Milner*, 131 S. Ct. at 1262, and thus the law "mandates a strong presumption in favor of disclosure." *EPIC v. Dep't of Justice*, 511 F. Supp. 2d 56, 64 (D.D.C. 2007) (internal citations omitted).

The FOIA includes exemptions from disclosure, "[b]ut these limited exemptions do not obscure the basic policy that disclosure, not secrecy, is the dominant objective of the Act." *Pub. Citizen, Inc. v. Rubber Mfrs. Ass'n,* 533 F.3d 810, 813 (D.C. Cir. 2008) (quoting *Nat'l Ass'n of Home Builders v. Norton*, 309 F.3d 26, 32 (D.C. Cir. 2002)) (internal quotation marks omitted). Therefore FOIA exemptions "must be narrowly construed." *Id*. "The statute's goal is broad disclosure, and the exemptions must be given a narrow compass." *Milner*, 131 S. Ct. at 1261 (internal citations omitted). Furthermore, "the burden is on the agency to sustain its action." 5 U.S.C. § 552(a)(4)(B); *see also EPIC v. Dep't of Homeland Security*, 384 F. Supp. 2d 100, 106 (D.D.C. 2005). Where the government has not carried this burden, summary judgment in favor

of the Plaintiff is appropriate. *See, e.g.*, *U.S. Dep't of Justice v. Tax Analysts*, 492 U.S. 136, 142 (1989); *Coastal States Gas Corp. v. Dep't of Energy*, 617 F.2d 854, 861 (D.C. Cir. 1980).

ARGUMENT

I. DHS May Not Withhold SOP 303 Under Exemption 7(E) Because it was Not Created "for Law Enforcement Investigations or Prosecutions"

An agency seeking to withhold records under Exemption 7(E) must satisfy two primary statutory elements. First, the record must be "compiled for law enforcement purposes." 5 U.S.C. § 552(b)(7). The D.C. Circuit has referred to this element as "the threshold requirement of Exemption 7." *See, e.g.*, *Tax Analysts v. I.R.S.*, 294 F.3d 71, 77 (D.C. Cir. 2002). Second, disclosure of the record must result in the harm recognized by Exemption 7(E): revealing either "techniques and procedures for law enforcement investigations or prosecutions," or "guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law." *See* 5 U.S.C. § 552(b)(7)(E).

These elements require different showings. *See, e.g.*, *Blackwell v. F.B.I.*, 646 F.3d 37, 40-42 (D.C. Cir. 2011) (analyzing first whether FBI files regarding the requester's prosecution were compiled for a law enforcement purpose, then whether their disclosure would reveal techniques or procedures for investigations or prosecutions). In particular, the threshold requirement of a law enforcement "purpose" is much broader than the requirement that disclosure reveal "techniques and procedures for law enforcement investigations or prosecutions." *See Pratt v. Webster*, 673 F.2d 408, 420 (D.C. Cir. 1982) (explaining that "Congress intended that 'law enforcement purpose' be broadly construed"); *Tax Analysts v. I.R.S.*, 294 F.3d 71, 79 (D.C. Cir. 2002) (noting that in 1986 Congress broadened Exemption 7's threshold requirement by "deleting any requirement that the information be 'investigatory'"). Accordingly, the Exemption 7 threshold covers law enforcement records unconnected to investigations or prosecutions. *See*

Id. ("It is clear that, under the amended threshold of Exemption 7, an agency may seek to block the disclosure of internal agency materials relating to guidelines, techniques, sources, and procedures for law enforcement investigations and prosecutions, even when the materials have not been compiled in the course of a specific investigation.").

The text of the statute, however, reveals that the rest of Exemption 7(E) may not be so easily satisfied. Indeed, many withholdings pass the "law enforcement purposes" requirement but fail the "techniques and procedures" requirement. *See, e.g.*, *Judicial Watch, Inc. v. U.S. Secret Serv.*, 579 F. Supp. 2d 182, 187-88 (D.D.C. 2008) ("The Court agrees with defendant that [Sensitive Security Record]s are compiled for law enforcement purposes. However, the Court cannot see how disclosure of the information plaintiff seeks would reveal techniques, procedures, or guidelines used by the Secret Service."); *Long v. U.S. Dep't of Justice*, 450 F. Supp. 2d 42, 79 *order amended on reconsideration*, 457 F. Supp. 2d 30 (D.D.C. 2006) *amended*, 479 F. Supp. 2d 23 (D.D.C. 2007) (finding that certain program category fields from databases of criminal investigations were compiled for law enforcement purposes but were not exempt under 7(E) because "the Department has failed to identify any law enforcement technique or procedure that would be disclosed upon release of the information").

Specifically, the harm recognized by Exemption 7(E) requires that law enforcement techniques, procedures, or guidelines be used for "law enforcement investigations or prosecutions." 5 U.S.C. § 552(b)(7)(E). Thus, it is not sufficient that the records in question simply disclose "techniques and procedures," or even that they disclose "techniques and procedures" related to "law enforcement purposes." Rather, the text of the statute plainly states that records must disclose "techniques and procedures *for law enforcement investigations or prosecutions.*" 5 U.S.C. § 552(b)(7)(E) (emphasis added); *see also Duncan v. Walker*, 533 U.S.

167, 174 (2001) ("It is our duty to give effect, if possible, to every clause and word of a statute.") (quotation marks omitted); *Cozen O'Connor v. U.S. Dep't of Treasury*, 570 F. Supp. 2d 749, 785 (E.D. Pa. 2008) ("[Exemption 7(E)] is construed literally."); *Peter S. Herrick's Customs & Int'l Trade Newsletter v. U.S. Customs & Border Prot.*, CIV.A. 04-00377 (JDB), 2006 WL 1826185, at *8 (D.D.C. June 30, 2006) ("[B]oth clauses of Exemption 7(E) require that the information shielded, at the very least, must be capable of use in law enforcement investigations or prosecutions.").

Here, DHS argues that SOP 303 satisfies Exemption 7's "law enforcement purpose" threshold requirement because it is a measure designed to prevent terrorism, specifically "a process for shutting down wireless networks to prevent bombings," Def.'s Mot. Summ. J., Dkt. 10, at 10. DHS also argues that SOP 303 satisfies the more specific, "techniques and procedures" requirements of Exemption 7(E) because it is a "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." Def.'s Mot. Summ. J., Dkt. 10, at 11-12. Despite the clear statutory requirements of 7(E), missing from DHS's argument is any claim that SOP 303 is a technique used "for law enforcement investigations or prosecutions." SOP 303 may indeed constitute a "technique," but it is a technique for "disabling a wireless telecommunications network," *id.* at 11, not a technique for a law enforcement investigation or prosecution. Although preventative measures may satisfy Exemption 7's threshold, they may not satisfy the rest of the exemption absent a connection to a law enforcement investigation or prosecution. DHS offers no explanation for how SOP 303 plays any role in investigations or prosecutions, and no conceivable connection exists. Indeed, DHS's enabling statute expressly gives primarily authority for terrorism investigations and prosecutions to other agencies. *See* 6

U.S.C. § 111(b)(2) ("[P]rimary responsibility for investigating and prosecuting acts of terrorism shall be vested not in the Department, but rather in Federal, State, and local law enforcement agencies with jurisdiction over the acts in question.")

DHS objects that requiring a connection to an investigation or prosecution reflects a "crabbed notion[] of law enforcement techniques." Def.'s Mot. Summ. J., Dkt. 10, at 12. Perhaps so, but that is the notion required by the text of the statute. DHS's interpretation effectively "tak[es] a red pen to the statute," *Milner v. Dep't of the Navy*, 562 U.S. __, 131 S. Ct. 1259, 1267 (2011), crossing out the words "for law enforcement investigations or prosecutions." Accordingly, its withholding under Exemption 7(E) is improper.

II. DHS Has Unlawfully Withheld SOP 303 Under Exemption 7(F)

A. DHS Misinterprets the "Any Individual" Standard

Under Exemption 7(F), information is protected where disclosure would "endanger the life or safety of any individual." 5 U.S.C. § 552(b)(7)(F). "In determining whether Exemption 7(F) applies, courts look for some nexus between disclosure and possible harm and whether deletions were narrowly made to avert the possibility of such harm." *Boehm v. F.B.I.*, No. 09-2173, 2013 WL 2477091 (D.D.C. June 10, 2013). While Exemption 7(F) "may be invoked to protect 'any individual' reasonably at risk of harm," the agency must focus its deletions "narrowly." *Long v. U.S. Dep't of Justice*, 450 F. Supp. 2d 42, 80 *order amended on reconsideration*, 457 F. Supp. 2d 30 (D.D.C. 2006) *amended*, 479 F. Supp. 2d 23 (D.D.C. 2007). Thus, where the Department of Justice "failed to demonstrate with sufficient specificity that releasing [extensive] information reasonably could be expected to endanger the life or physical safety of any individual," the agency was not permitted to assert Exemption 7(F). *Id.* The Court noted of the DOJ, "[I]t offers little more than conclusory assertions that disclosure will increase

the chances that third parties will be harmed in some way. Such unsupported speculation cannot serve as a justification for withholding information under Exemption 7(F)." *Id*.

Generally, this court has defined Exemption 7(F) as the "exemption [that] affords broad protection to the identities of individuals mentioned in law enforcement files ..., including any individual reasonably at risk of harm." *Brestle v. Lappin*, No. 11-1771, 2013 WL 3107486 (D.D.C. June 20, 2013), (*citing Quinto v. DOJ*, 711 F.Supp.2d 1, 8 (D.D.C. 2010)). Thus, in *Brestle*, *Quinto*, and *Boehm*, 7(F) was properly asserted where releasing the records would reveal the identity of police informants, who might then be at risk of retaliation by either the plaintiff or some member of the public. *Brestle*, No.11-1771, at *8; *Quinto*, 711 F.Supp.2d at 8; *Boehm*, No. 09-2173, at *22. The connection between individuals named in law enforcement records, their participation in informant activities, and a risk of retaliation if their names were revealed all form a "nexus between disclosure and possible harm," meriting "narrow deletions to avert the possibility of such harm." *Boehm*, No. 09-2173, at *22. DHS cannot form that nexus here.

The "individuals" that DHS refers to in its Motion for Summary Judgment are "individuals near unexploded bombs." Def.'s Mot. Summ. J., Dkt. 10, at 15. This identification of "individuals" is insufficient. According to DHS, there are no identified individuals "mentioned in law enforcement files" whom the agency seeks to protect by invoking Exemption 7(F). As a result, DHS cannot establish the "nexus" required between disclosure of the individuals mentioned in their records and a risk of harm to those individuals. The "nexus" test requires that the agency link the disclosure of the "individual's" identity to a risk of harm. DHS cannot make that link, since the agency has identified no individuals whose identities it seeks to protect under Exemption 7(F).

DHS cites *Amuso* for the proposition that "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. DOJ*, 600 F. Supp. 2d 78, 101 (D.D.C. 2009). However, Exemption 7(F) must apply to individuals who can be identified with some degree of specificity. In *ACLU v. Dep't of Defense*, 543 F. 3d 59 (2d. Cir. 2008), the court noted that "the phrase 'any individual' in exemption 7(F) may be flexible, but it is not vacuous." *Id*. at 67. The court continued:

> [I]t is true that the statute does not read 'any *named* individual,' and we thus understand it to include individuals identified in some way other than by name – such as, for example, being identified as family members or coworkers of a named individual, or some similarly small and specific group. This does not, however, mean that the individual contemplated by exemption 7(F) need not be identified at all, or may be identified as a member of a vast population.

Id. at 67-8. The Second Circuit explained that "by requiring a showing of danger to an individual, Congress provided a constraint limiting exemption 7(F) to its intended scope – the protection of individuals subject to a *non-speculative* risk of harm incident to a law enforcement investigation." *ACLU*, 543 F. 3d. at 80.

Contrary to DHS's analysis, *Amuso* does not permit an agency to forgo the "nexus" test and simply identify a possible risk without also identifying the individual whom disclosure would put at risk. The agency need not identify these individuals by name, but it must nevertheless show that there are certain individuals in need of 7(F) protection. *Id*. All of DHS's "individuals" are hypothetical; there are no names or identifying characteristics about DHS's "individuals" that would put them in any danger if that information were released. In fact, the Second Circuit has explicitly noted that the "individual" at issue may not be "a member of a vast population." *Id.* at 68. A statute written to protect individuals from risk of harm if their law enforcement activity were exposed cannot also support an interpretation that prevents an agency

from disclosing documents that do not name or even contemplate any individuals. DHS has misunderstood the function of the 7(F) exemption, and cannot withhold SOP 303 under this provision.

B. DHS Improperly Relies on the Holding in *Living Rivers*

DHS attempts to avoid the fact that it cannot identify any "individual" for the purpose of the nexus test by relying on an analogy to the *Living Rivers* case in the Utah District Court. However, the agency mischaracterizes the holding of the *Living Rivers* decision and rests its argument on a faulty analogy. In *Living Rivers*, the court held that the Bureau of Reclamation's properly withheld maps that described the effects of inundation on "the downstream areas that would be flooded by a breach of Hoover Dam or Glen Canyon Dam." *Living Rivers, Inc. v. U.S. Bureau of Reclamation*, 272 F. Supp. 2d 1313, 1321 (D. Utah 2003). Since terrorists could use the geographical data provided by the maps to plan attacks on downstream areas, the court held that release of the maps could jeopardize the safety of the downstream population. *Id*. at 1322. DHS analogizes the American public to the downstream population in *Living Rivers*, asserting that "[r]eleasing information regarding this protocol would enable 'bad actors' to blunt its usefulness . . . 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." Def.'s Mot. Summ. J., Dkt. 10, at 15. This analogy fails, however, since the population at risk in *Living Rivers*' was a specific, identifiable group, and the population that DHS seeks to protect in this case is some hypothetical group of the public. *Living Rivers* differs from most successful 7(F) withholdings in that the "individuals" protected by the withholding were not at risk from a specific existing threat. *Id*. at 1321. The "terrorists" contemplated in *Living Rivers* were hypothetical. However, the population at risk was specific and identifiable. Unlike the

instant case, the government in *Living Rivers* identified the specific region whose inhabitants would be affected by a terrorist attack on the dams. In this case, not only is the activity hypothetical, but so too are the "individuals" -- the affected population could be any part of the American public – essentially, the "identified" population is the entire United States.

III. DHS Has Failed to Segregate and Release Non-Exempt Portions of Records

The FOIA requires the government to disclose any "reasonably segregable portion of a record." 5 U.S.C. § 552(b); *see Oglesby v. United States Dep't of the Army*, 79 F.3d 1172, 1176 (D.C. Cir. 1996) ("If a document contains exempt information, the agency must still release 'any reasonably segregable portion' after deletion of the nondisclosable portions.") (citation omitted). "The 'segregability' requirement applies to all documents and all exemptions in the FOIA." *Ctr. for Auto Safety v. Envtl. Prot. Agency*, 731 F.2d 16, 21 (D.C. Cir. 1984). As with all parts of FOIA litigation, the burden is on the government to "provide a detailed justification for its non-segregability." *Johnson v. Exec. Office for U.S. Attorneys*, 310 F.3d 771, 776 (D.C. Cir. 2002) (internal quotation marks omitted). This includes "a statement of [the government's] reasons," and a "descri[ption of] what proportion of the information in a document is non-exempt and how that material is dispersed throughout the document." *Mead Data Cent., Inc. v. Dep't of Air Force*, 566 F.2d 242, 261 (D.C. Cir. 1977). Simply claiming that a segregability review has been conducted is insufficient. *Oglesby*, 79 F.3d at 1180. Finally, district courts have an "affirmative duty to consider the segregability issue *sua sponte*." *Trans-Pac. Policing Agreement v. U.S. Customs Serv.*, 177 F.3d 1022, 1028 (D.C. Cir. 1999).

Here, DHS failed to perform an adequate segregability analysis. DHS released a copy of SOP 303 to EPIC that was almost entirely redacted, stating that "[n]o other segments of the document could be released without compromising the interests protected by the exemptions

invoked by DHS." Def.'s Mot. Summ. J., Dkt. 10, at 15 (citing Holzer Decl. ¶ 22). But this statement is a conclusion, not an explanation. "[U]nless the segregability provision of the FOIA is to be nothing more than a precatory precept, agencies must be required to provide *the reasons behind their conclusions* in order that they may be challenged by FOIA plaintiffs and reviewed by the courts." *Mead Data Cent., Inc.*, 566 F.2d at 261 (emphasis added). DHS has provided nothing more than "empty invocation[s] of the segregability standard" that the Court should reject. *Judicial Watch, Inc. v. Dep't of Homeland Sec.*, No. 11-00604, 2012 WL 251914, at *12 (D.D.C. Jan. 27, 2012).

Although EPIC does not bear the burden of finding segregable material, at the very least, the predetermined shutdown questions contained within SOP 303 should be segregated and released. This portion of the SOP consists of a "pre-determined series of questions that determines if a shutdown is necessary . . . ." Holzer Decl., Dkt. 10-2, ¶ 21. Even accepting DHS's arguments regarding Exemptions 7(E) and 7(F), the questions are plainly not law enforcement techniques. Under the definition proffered by the agency, a "technique" is "a particular way of doing or of going about the accomplishment of something." Def.'s Mot. Summ. J., Dkt. 10, at 12; *see also Allard K. Lowenstein Int'l Human Rights Project v. Dep't of Homeland Sec.*, 626 F.3d 678, 680-82 (2d Cir. 2010) (referring to the same definition of "technique"). The shutdown questions, however, are not a means of accomplishing a wireless communications shutdown; they are the means of determining whether to employ a shutdown in the first place. In other words, the shutdown questions are matters of general policy that precede the use of any specific shutdown technique.

Furthermore, release of the predetermined shutdown questions would cause no harm to law enforcement interests. Even if a technique or procedure was both compiled for law

enforcement purposes and used for investigation or prosecution, the government must still demonstrate that harm would result from its disclosure. In the D.C. Circuit, this harm typically occurs where disclosure would allow bad actors to evade, defeat, or otherwise circumvent the techniques, thereby reducing their effectiveness. *See Blackwell v. F.B.I.*, 646 F.3d 37 (D.C. Cir. 2011) (holding that techniques for computer forensic examination data collection were exempt because disclosure would reduce their effectiveness by "exposing computer forensic vulnerabilities" and "enable[ing] criminals to employ countermeasures to avoid detection" (internal quotation marks omitted)); *James v. U.S. Customs and Border Prot.*, 549 F. Supp. 2d 1, 10 (D.D.C. 2008) (withholding the specific search techniques used on requester because disclosure would "assist in subverting the effectiveness of a particular investigative technique . . . and could enable smugglers of contraband to employ measures to neutralize those techniques" (internal quotation marks omitted)); *Hidalgo v. Fed. Bureau of Investigation*, 541 F. Supp. 2d 250, 254 (D.D.C. 2008) (explaining that Exemption 7(E) only allows "information about law enforcement techniques to be withheld when publication would allow perpetrators to avoid them . . .").

Here, bad actors would not be able to use the predetermined shutdown questions alone to defeat the shutdown of wireless networks because they would still lack necessary information contained in the rest of SOP 303. In many cases, disclosure is permitted where interference with or circumvention of a technique would require additional, undisclosed information. *See, e.g.*, *Island Film, S.A. v. Dep't of the Treasury*, 869 F. Supp. 2d 123, 138 (D.D.C. 2012) (rejecting withholding of database printouts because "the documents themselves do not describe OFAC's procedure for accessing certain databases in the course of its investigations"); *Families for Freedom v. U.S. Customs & Border Prot.*, 797 F. Supp. 2d 375, 391 (S.D.N.Y. 2011) (disclosing

information about a specific border control station because it did not contain "arrest statistics for *each station* within the Buffalo sector, which could theoretically aid circumvention of the law by publicizing the relative activity or success of Border Patrol agents in effecting apprehensions at each station"); *Pub. Employees for Envtl. Responsibility (Peer), Rocky Mountain Chapter v. U.S. E.P.A.*, 978 F. Supp. 955, 963 (D. Colo. 1997) (disclosing material in investigative reports because it "discusses coding of confidential sources but does so without alerting the reader how to decipher the code"). SOP 303 contains multiple parts, including (1) the predetermined series of questions that determine if a shutdown is necessary, (2) authentication methods, and (3) the step-by-step shutdown process itself. *See* Holzer Decl. ¶ 25. Releasing the predetermined shutdown questions would disclose only one part of the SOP, but effectively circumventing a shutdown would require information about the entire procedure. In fact, the predetermined shutdown questions are akin to broad policy regarding the appropriate circumstances for wireless shutdown that is too general to enable interference with any specific network deactivation. Accordingly, they should be segregated and released.

CONCLUSION

For the foregoing reasons, the Court should deny the government's motion for summary judgment and grant Plaintiffs' cross-motion for summary judgment. At a minimum, the Court should order DHS to conduct an adequate segregability review of SOP 303.

Dated: July 26, 2013

Respectfully submitted,

MARC ROTENBERG
President and Executive Director

/s/ Ginger P. McCall
GINGER P. MCCALL
(DC Bar No. 1001104)

DAVID JACOBS[*]
JULIA HORWITZ[**]
Electronic Privacy
Information Center
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009
Telephone: (202) 483-1140
Fax: (202) 483-1248
mccall@epic.org

Attorneys for Plaintiff

[*] Admitted to practice in New York, admission pending in D.C.
[**] Admitted to practice in Maryland, admission pending in D.C.