

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

<hr/>)
ELECTRONIC PRIVACY INFORMATION)
CENTER)
)
Plaintiff,)
)
v.)
	Civil Action No. 13-00260 (JEB))
)
U.S. DEPARTMENT OF)
HOMELAND SECURITY)
)
Defendant.)
<hr/>)

**PLAINTIFF’S REPLY BRIEF IN SUPPORT OF CROSS-MOTION FOR SUMMARY
JUDGMENT**

INTRODUCTION

Standard Operating Procedure 303 (“SOP 303”) sets out a protocol for deactivating wireless communications networks. Wireless networks are the essential backbone of modern communications services, allowing individuals to send and receive email and text messages, search the Internet, organize political activity, communicate with others, and contact emergency services, such as 911. As EPIC explained in its initial brief, SOP 303 “threatens both freedom of speech and public safety” by preventing a large number of individuals from engaging in wireless communications. Despite the serious constitutional implications of SOP 303 and the public interest in knowing “what the Government is up to,” *Nat’l Archives & Records Admin. v. Favish*, 541 U.S. 157, 171-72 (2004), DHS has chosen to withhold SOP 303 under Exemptions 7(E) and 7(F). In doing so, the agency has mischaracterized the scope of SOP 303 and improperly distorted the meaning of those exemptions.

Exemption 7(E) applies to law enforcement records that would “disclose techniques and

procedures for law enforcement investigations or prosecutions” 5 U.S.C. § 552(b)(7)(E). DHS has advanced a reading of this exemption that ignores the plain meaning of the phrase “for law enforcement investigations or prosecutions,” and thus would permit law enforcement records to be withheld when there is no connection to any investigation, or a connection so attenuated as to engulf the other FOIA exemptions. Exemption 7(F) applies to law enforcement records where disclosure “could reasonably be expected to endanger the life or safety of any individual.” 5 U.S.C. § 552(b)(7)(F). Again, DHS adopts an overly broad reading of the exemption by applying it to protect an unidentified population in an unspecified place at an indeterminate time from the risk posed by a hypothetical bomb. Finally, DHS has not adequately justified its refusal to segregate and disclose certain, logically-divisible parts, such as the predetermined shutdown questions.

ARGUMENT

I. DHS is Improperly Withholding SOP 303 Under Exemption 7(E)

DHS plainly misstates the purpose of Exemption 7(E). In addition to the threshold requirement of a valid law enforcement purpose, Exemption 7(E) requires that the records at issue “disclose techniques and procedures for law enforcement investigations or prosecutions” 5 U.S.C. § 552(b)(7)(E). The text of the statute clearly requires that the “techniques and procedures” be used not just for any law enforcement purpose, but *for investigations or prosecutions*. An investigation is a process of inquiring into or tracking down through inquiry. *Black’s Law Dictionary* 825 (6th ed.1990); *see also Webster’s Third New Int’l Dictionary Unabridged* 1189 (2002) (defining “investigation” as a “detailed examination . . . study . . . research . . . [or] official probe”). Accordingly, Exemption 7(E) has been applied to protect records related to the process of an inquiry, such as methods of gathering or organizing

information. *See, e.g., Lewis-Bey v. DOJ*, 595 F. Supp. 2d 120, 137 (D.D.C. 2009) (details of electronic surveillance techniques); *Edmonds v. FBI*, 272 F. Supp. 2d 35, 56 (D.D.C. 2003) (polygraph information); *Judicial Watch, Inc. v. U.S. Dep't. of State*, 650 F. Supp. 2d 28 (D.D.C. 2009) (notes regarding investigations of criminal wrongdoing by government employees).

SOP 303 plainly is not a technique for inquiry; it is a technique for deactivating wireless communication networks. In its reply brief, DHS imagines that SOP 303 might nevertheless also be an investigatory technique because it prevents bombs from exploding, and exploding bombs occasionally destroy evidence. *See* Def.'s Reply and Opp., Dkt. 13, at 5-6 ("Preventing explosives from detonating preserves evidence—*i.e.*, the bomb and its surroundings—and, thereby, facilitates the investigation into who built and placed the bomb. . . . Thus, SOP 303 supports efforts to identify, through investigation, those responsible for the creation and placement of a bomb"). Of course, nowhere in DHS's initial brief, the declaration of James Holzer, or the NSTAC reports initially describing SOP 303 is there even a hint of such an investigatory purpose. This is because no ordinary speaker of the English language, when faced with SOP 303, would describe it as a technique for investigating or prosecuting unlawful activity.

Furthermore, DHS's proposed interpretation of the key term "investigation" in 7(E) would create an exemption without limits. From the perspective of a law enforcement agency, almost anything could be said to "support" or "facilitate" investigations. But the fact that a technique might indirectly create conditions conducive, in some circumstances that can be imagined, to a future investigation does not automatically convert it into a technique *for* investigation. Otherwise, the court in *Living Rivers, Inc. v. U.S. Bureau of Reclamation*, 272 F. Supp. 2d 1313 (D. Utah 2003)—a case that DHS relies upon heavily—would have been forced

to conclude that inundation maps revealing the effects of dam failure were techniques for law enforcement investigations. Withholding the inundation maps decreases the chance that bad actors will successfully execute an attack by preventing them from learning useful information such as the relative infrastructural vulnerabilities, the priorities of security staff, and emergency response plans. *See id.* at 1315-16. Evidence, such as bombs, is more likely to be preserved during a failed attack. Therefore, inundation maps support efforts to investigate those responsible for targeting a dam. Similarly, the court in *Raheer v. Fed. Bureau of Prisons*, No. 09-526-ST, 2011 WL 2014875 (D. Or. May 24, 2011), would have had to conclude that records containing prison staffing patterns and internal security procedures were also techniques for law enforcement investigations. Withholding such records helps prevent inmates from escaping. *See id.* at *9. Inmates are a potential source of evidence. Therefore, the records support efforts to identify and investigate those responsible for crimes. And even information related to the funding of confidential informants would have to be considered a technique for law enforcement investigation. *But see Hidalgo v. F.B.I.*, 541 F. Supp. 2d 250, 253-54 (D.D.C. 2008). Such funding information prevents criminals from inflating the price point of the market for informants. *See id.* at 254. Because law enforcement agencies have limited resources, money saved on informants could be spent on other investigative techniques. Therefore, informant funding information also “supports” law enforcement investigations.

DHS’s expansive reading of Exemption 7(E) would also render other FOIA exemptions superfluous. Exemption 7(A), for example, protects law-enforcement records if disclosure “could reasonably be expected to interfere with enforcement proceedings.” 5 U.S.C § 552(b)(7)(A). Courts have interpreted Exemption 7(A) to permit withholding in order to preserve evidence. *See, e.g., Juarez v. DOJ*, 518 F.3d 54, 58 (D.C. Cir. 2008) (protecting records under Exemption

7(A) where disclosure “would compromise the investigation as it could lead to destruction of evidence”); *Ctr. for Nat’l Sec. Studies v. DOJ*, 331 F.3d 918, 929 (D.C. Cir. 2003) (reviewing cases that have found “evidence tampering” concerns sufficient to justify Exemption 7(A)). But under DHS’s reading, there would be no need for Exemption 7(A) in such circumstances; any record that tends to facilitate a subsequent investigation would be protected under Exemption 7(E). Thus, DHS’s theory would invalidate the holdings of numerous Exemption 7(E) cases, engulf other exemptions, and turn FOIA from a “disclosure statute” into a “withholding statute.” *Cf. EPA v. Mink*, 410 U.S. 73, 79 (1973).

DHS’s primary argument, however, is that it need not detail the manner in which SOP 303 is a technique for law enforcement investigations or prosecutions because such a requirement reflects a “cramped understanding” of Exemption 7(F). Def.’s Reply and Opp., Dkt. 13, at 2. DHS begins with a discussion of the purpose and interpretive principles applicable to FOIA. *Id.* at 3. But none of FOIA’s “other important interpretive principles” exempt it from the “cardinal canon” of statutory interpretation: that “courts must presume that a legislature says in a statute what it means and means in a statute what it says there.” *Connecticut Nat. Bank v. Germain*, 503 U.S. 249, 253-54 (1992). Even in the FOIA context, “proper deference must be paid to the plain meaning rule.” *Symons v. Chrysler Corp. Loan Guarantee Bd.*, 670 F.2d 238, 241 (D.C. Cir. 1981) (citing *Consumers Union of the United States, Inc., v. Heimann*, 589 F.2d 531, 533 (D.C. Cir. 1978)). Here, Exemption 7(E) plainly requires that the “technique” in question be “for investigations”—that is, for the process of inquiring into or tracking down through inquiry. DHS evidently wishes that Congress had written a different statute, one with a relaxed requirement for techniques and procedures. But the statute that Congress actually wrote requires that techniques and procedures be “for law enforcement investigations or prosecutions,”

and the Court must give effect to these words. *See Donnelly v. F.A.A.*, 411 F.3d 267, 271 (D.C. Cir. 2005) (“We must strive to interpret a statute to give meaning to every clause and word, and certainly not to treat an entire subsection as mere surplusage.”). And there is nothing “cramped” or “wooden” about giving these words the effect of their plain meaning. FOIA provides ample opportunities to withhold documents, such as SOP 303, that the government seeks to withhold despite the absence of a direct connection to a law enforcement investigation. Exemption 7(F), although inapplicable in this case, protects law-enforcement documents where disclosure “could reasonably be expected to endanger the life or physical safety of any individual.” 5 U.S.C. § 552(b)(7)(F). Exemption 3, which exempts records that other statutes protect from disclosure, “offer[s] Congress an established, streamlined method to authorize the withholding of specific records that FOIA would not otherwise protect.” *Milner v. Dep’t of Navy*, 562 U.S. ___, 131 S. Ct. 1259, 1271 (2011). Additionally, Exemption 1 could protect SOP 303 if it were properly classified. *See* 5 U.S.C. § 552(b)(1).

In support of its text-light reading of Exemption 7(E), DHS leans heavily on *U.S. News & World Report v. Dep’t of Treasury*, 1986 U.S. Dist. LEXIS 27634 (D.D.C. Mar. 26, 1986), an unpublished district court opinion from 1986. *See* Def.’s Reply and Opp., Dkt. 13, at 4-5. In *U.S. News*, the court considered the application of Exemption 7(E) to “information concerning the [presidential parade] limousines’ specifications, price, weight, product numbers, equipment, parts and general pricing information.” 1986 U.S. Dist. LEXIS 27634, at *3-4. The court held that Exemption 7(E) applied to the specifications of the presidential limousines, but did not apply to “general pricing information” about the vehicles. *Id.* at *8. *U.S. News*, however, cannot bear the weight that DHS puts on it for several reasons. First, the court’s holding was limited to the Secret Service. The holding rested on the “unique nature” of the Secret Service’s function, which

centers around “protect[ing] persons such as the President from both known and unknown threats.” *Id.* at *6. In contrast to the uniquely protective mission of the Secret Service, the National Coordinating Center (“NCC”)—which developed SOP 303—performs a wide variety of functions. The NCC is a “joint industry-government telecommunications entity established . . . to assist in the initiation, coordination, restoration and reconstitution of national security and emergency preparedness telecommunications services or facilities under all conditions of crisis or emergency.” 47 C.F.R. § 201.2. If the court in *U.S. News* meant anything when it described the Secret Service as “unique,” then a public-private telecommunications partnership is not eligible for the same kind of special treatment as the Secret Service, a pure law enforcement agency with over a century of experience protecting presidents and other heads of state and government.

Second, *U.S. News* was decided long before the Supreme Court ruled in *Milner v. Department of Navy*. *Milner* made clear the importance of textual fidelity in FOIA matters. In *Milner*, the Court held that the Navy’s use of Exemption 2 to withhold maps used to help store explosives at a naval base could not be squared with the plain text of the statute. 562 U.S. ___, 131 S. Ct. 1259 (2011). In rejecting the Navy’s “text-light” approach to FOIA interpretation, the Court noted that “the only way to arrive at [the Navy’s interpretation] is by taking a red pen to the statute—‘cutting out some’ words and ‘pasting in others’ until little of the actual provision remains.” *Id.* at 1267 (citing *Elliott v. Dep’t of Agric.*, 596 F.3d 842, 845 (D.C. Cir. 2010)). Similarly, the only way to arrive at DHS’s interpretation of Exemption 7(E) is to “tak[e] a red pen to the statute” and cross out the phrase “for law enforcement investigations or prosecutions.” Although *Milner* involved a different exemption than this case, the interpretative rule concerning the text of FOIA is controlling. The approach urged by DHS, relying on *U.S. News*, a district

court opinion from twenty years ago, is unsustainable in light of *Milner*. This Court “ha[s] no warrant to ignore clear statutory language on the ground that other courts have done so.” *Id.* at 1268.

II. DHS is Improperly Withholding SOP 303 Under Exemption 7(F)

Contrary to the government’s assertions, Exemption 7(F) does not support the withholding of SOP 303. As EPIC explained in its opening brief, an agency may assert Exemption 7(F) where disclosure “could reasonably be expected to endanger the life or safety of any individual.” 5 U.S.C. § 552(b)(7)(F). “Any individual” may “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.” *ACLU v. Dep’t of Defense*, 543 F. 3d 59, 67-68 (2d.Cir. 2008), *vacated*, 558 U.S. 1042 (2009). The fact that the “individuals” need not be identified by name “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 81. Further, as EPIC explained, a disclosure of information can “reasonably be expected to endanger to life or safety” of the individual when the agency can demonstrate to the court “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).

DHS misses the crucial point that the courts cannot apply the “nexus” test if the category of “individuals” is too broad to determine whether the deletions are “narrowly made to avert the possibility of harm.” *Id.* The “any individual” standard is thus linked to the “nexus” test in that the scope of withheld information cannot be assessed for appropriate narrowness if the possibility of harm does not just affect “any individual,” but *every* individual. As a result, DHS

has not satisfied the standards for withholding SOP 303. DHS asserts that SOP 303 must be withheld to protect anyone “within the blast radius of a remotely detonated bomb.” Def.’s Reply and Opp., Dkt. 13, at 11. These hypothetical bombs, however, could materialize at any time, in any place, and affect anyone in the United States. Thus, the “individuals” identified by DHS are “members of a vast population,” *ACLU*, 543 F. 3d, at 81. Courts cannot apply the “nexus” test to gauge the possibility of speculative harm on a “vast population” of people, effectively rendering DHS’s assertion of 7(F) unreviewable. Thus, the government’s withholding under Exemption 7(F) is improper.

In an attempt to demonstrate the breadth of the “any individual” standard, DHS cites four cases in which “information other than individuals’ identities” were withheld pursuant to Exemption 7(F). However, in each of these cases, the nexus between the information withheld under the statute and the risk of harm to be averted are much more narrowly construed than DHS’s characterization would allow.

In the first case, *Zander v. Dep’t of Justice*, 885 F. Supp. 2d 1 (D.D.C. 2012), this court held that the exemption most clearly applied to information that could expose law enforcement officers to violence by inmates. In *Zander*, the Bureau of Prisons properly withheld a video, under Exemption 7(F), that showed officers forcibly removing the defendant from his prison cell. The Bureau of Prisons claimed that releasing a video of forcible removal techniques to the public could endanger the lives and safety of Bureau of Prisons officers who plan to use those techniques in the future. *Id.* at 7-8. This court held that “that the video [wa]s properly withheld under FOIA exemption 7(F). Exemption 7(F) most clearly applies to protect law enforcement officials from disclosure of information that could prove threatening to them.” *Id.* at 7. In that case, the government showed a close nexus between the potential threat and the disclosure of

information. BOP could identify not only the group of individuals potentially at risk (police officers working in prisons) but also the source of the potential threat (the prisoners themselves), the location of the potential attack (the prisons), and the scenario in which the attack would occur (forcible removal of prisoners from their cells). Since the release of the videos would have provided potential criminals with unique insight into law enforcement officers' techniques, this court found that the nexus between disclosure of the information and risk of harm to individuals was "abundantly reasonable." *Id.*

Two other cases that DHS invokes involve the withholding of inundation maps pursuant to Exemption 7(F). In *Pub. Employees for Evtl. Responsibility v. U.S. Section Int'l Boundary & Water Comm'n*, 839 F. Supp. 2d 304 (D.D.C. 2012), this court held that where inundation maps "identify and delineate areas that would be affected by floods in the event of dam failure," and "show estimated travel times for flood progression as well as peak elevation for waters in the event of dam failure... release of such maps could increase the risk of terrorist attack on the dams." *Id.* at 328. The government in *PEER* was able to demonstrate a nexus between the release of information and the possibility of a terrorist attack; the location of the potential attack was clearly defined, the population affected could be reasonably identified, and even the amount of time that it would take for the harm to occur after the potential attack was articulated in the "estimated travel times for flood progression" included in the maps. The specificity with which the government could identify the time, place, and nature of the attack justified its withholding.

The other case pertaining to inundation maps is *Living Rivers*, 272 F. Supp. 2d. Both parties have already briefed this case extensively, so little analysis remains. *Living Rivers* preceded *PEER*, and served as the basis for much of this court's analysis. *Id.* Both cases involved the withholding of inundation maps under Exemption 7(F), and in both cases the courts found

that the release of specific information regarding the risk posed to downstream inhabitants of major dams could facilitate acts of terrorism. As in *PEER*, most of the specifics of the threat posed by disclosure of the inundation maps were clear to the government and the court: the “individuals” at risk were the downstream inhabitants of the dam regions, location of the attacks would be the dams themselves, the time it would take for the attacks to take place were articulated on the inundation maps, and the mechanism for causing harm was the flooding described on the withheld documents. DHS attempts to respond to EPIC’s analysis of *Living Rivers* by suggesting, “the group of people who would be affected by attacks on the immense Hoover and Glen Canyon Dams cannot reasonably be described as ‘specific’ and ‘identifiable.’” The group would include not only residents, but people passing through the large downstream areas on business or pleasure. And, in any event, not all residents would be there at any given time.” Dkt. 13 at 11. However, DHS’s explanation actually underscores the extent to which the *Living Rivers* population is “identifiable.” The crucial inquiry when assessing Exemption 7(F) is not whether the government seeks to protect a narrow group of individuals, but instead whether the government seeks to protect a group of narrowly *defined* individuals. Thus, the fact that DHS is able to offer a more detailed description of the group at risk in *Living Rivers* demonstrates the applicability of Exemption 7(F) in that case; the government was able to meet its burden to describe the at-risk “individuals” with some specificity because the location of the dams, the area that would be affected by an attack, and the various populations that would be affected by an attack were readily identifiable.

Finally, contrary to DHS’s assertion, *Peter S. Herrick’s Customs & Int’l Trade Newsletter v. U.S. Customs & Border Protection*, 2006 WL 1826185 (D.D.C. June 30, 2006) does not stand for the proposition that an agency may avoid identifying an at-risk group of

individuals under Exemption 7(F). In *Peter S. Herrick's*, this court found that CPB properly applied 7(F) to withhold “(1) information regarding the seizure, location, placement, storage, possession, physical security, inventory, testing, and evaluation of, and access to, seized contraband; and (2) the titles of employees, groups, and task forces responsible for the seizure, storage, possession, physical security, inventory, testing and evaluation of seized contraband.” *Id.* at *9. The information in the first category of withheld documents – the location of seized contraband – already demonstrates a clear nexus with the risk of potential harm to identifiable individuals. Just as the officers in *Zander* would have been put at risk by prisoners having access to their forcible removal techniques, so would CBP officers be put at risk of potential harm by purveyors of illegal contraband who could gain insight into officer’s seizure and storage techniques. Moreover, the information in the second category – the titles, groups and task forces responsible for carrying out these tasks – would place Customs officers at further risk. Since the group of individuals to be protected is easily identified as the Customs officers, and the information withheld would expose the identities of and techniques used by the Customs officers, the withheld information constitutes a “narrowly made” deletion.

The government’s proposed application of Exemption 7(F) would effectively negate the “nexus” test that the courts have developed. In each of the cases cited by the government that test is met. But it could not even be applied in the present case. The nexus test assesses the effect of disclosure on a person or set of people; where disclosure is likely to threaten the safety of those individuals, the 7(F) exemption is properly applied. Here, the potential harm in disclosure is not tied to a particular location or timeframe, and the at-risk population is broad enough to encompass every person in the US. Therefore, the potential harm is too vague and the at-risk population is too broad to assess.

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

An adequate segregability justification entails “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). This “detailed justification,” must be made through an agency’s affidavits. *See Johnson v. Executive Office for U.S. Attorneys*, 310 F.3d 771, 776 (D.C. Cir. 2002) (holding that agency’s affidavits, combined with a Vaughn index, were sufficient to meet the segregability standard).

DHS’s single-sentence segregability justification fails to meet FOIA’s requirements. *See* Holzer Decl., Dkt. 10-2, ¶ 22 (“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.”). Although DHS describes the “detailed justification” given for withholding SOP 303, *see* Def.’s Reply and Opp., Dkt. 13, at 13, this explanation applies only to SOP 303 *as a whole*. As explained in EPIC’s earlier brief, and as DHS admits, SOP 303 contains multiple parts including the predetermined series of questions that determine if a shutdown is necessary; authentication methods; and the step-by-step shutdown process itself. When a document contains “logically divisible sections for which the proportion and distribution description [of nonexempt material] would differ significantly,” then an agency should describe the document “by section rather than as a whole.” *Mead Data Cent.*, 566 F.2d at 261. Here, a detailed justification would have required DHS to explain, for each of the distinct parts, why that part could not be segregated and released. This is especially true given that EPIC singled out several of these parts, such as the predetermined “series of questions,” in its initial FOIA request. *See* EPIC FOIA Request, Dkt. 10-1, at 4.

Even assuming that SOP 303 as whole warrants protection under Exemptions 7(E) and 7(F), it does not follow that each of its logically distinct parts deserves similar treatment. Some of those parts—for example, the “pre-determined series of questions that determines if a shutdown is necessary”—are neither techniques for law enforcement investigations nor harmful if disclosed. First, the pre-determined shutdown questions are not techniques *for law enforcement investigations or prosecutions*, as required by the plain text of Exemption 7(E), for the reasons described in Part I above. DHS is right in claiming that the pre-determined shutdown questions are “a particular way of doing or going about the accomplishment of something” Def.’s Reply and Opp., Dkt. 13, at 15 (quoting *Webster’s Third New Int’l Dictionary* (1986)). What DHS does not claim, and cannot claim, is that the “something” being accomplished is a law enforcement investigation or prosecution.

Instead, the predetermined shutdown questions are akin to an agency’s public policy. DHS claims that there is “no support available” for treating the series of shutdown questions as policy. Def.’s Reply and Opp., Dkt. 13, at 15. The pre-determined shutdown questions, however, are the product of agency decision-making; they are generally applicable to the U.S. public; they consider various public welfare factors, such as “public safety hazards” Holzer Decl., Dkt. 10-2, at 9; and they contain the standards by which DHS imposes a prior restraint on the speech of a large number of individuals. This satisfies the ordinary meaning of the term “policy.” *See Black’s Law Dictionary* (9th ed. 2009) (defining “policy” as “[t]he general principles by which a government is guided in its management of public affairs.”); *Webster’s Third New Internat’l Dictionary* 1754 (1981) (defining “policy” as “a definite course or method of action and selected from among alternatives and in the light of given conditions to guide and determine present and future decisions.”). Accordingly, the shutdown questions may not be withheld under FOIA. *See*

Don Ray Drive-A-Way Co. of California, Inc. v. Skinner, 785 F. Supp. 198, 200 (D.D.C. 1992) (holding Exemption 7(E) inapplicable to the algorithm used to determine a motor carrier's safety rating because “It is regularly followed in all ratings; it controls final agency action subject to review; and it has the same status as regulations or agency law.”); *cf. Public Citizen, Inc. v. Office of Management and Budget*, 598 F.3d 865 (D.C. Cir. 2010) (ordering disclosure of “[d]ocuments reflecting OMB's formal or informal policy on how it carries out its responsibilities”); *Coastal States Gas Corp. v. Dep't of Energy*, 617 F.2d 854, 869 (D.C. Cir. 1980) (FOIA does not protect documents reflecting agency guidance or precedent applied by agency staff in their dealings with the public).

Second, DHS has not established that harm would result from release of the predetermined shutdown questions. Both Exemption 7(E) and 7(F) protect against some type of consequential harm: in the case of Exemption 7(F), the harm is “endanger[ment] of the life or physical safety of any individual,” 5 U.S.C. § 552(b)(7)(F); in the case of Exemption 7(E), the harm is evasion or interference with a particular technique or procedure. *See, e.g., James v. U.S. Customs and Border Prot.*, 549 F. Supp. 2d 1, 10 (D.D.C. 2008).¹ Both of these harms—endangerment and interference—require bad actors to know *when*, *where*, and *how* a wireless deactivation would be accomplished. The shutdown questions alone would not provide the necessary information. Courts routinely allow disclosure of certain information where endangerment or interference requires information contained in other, withheld records. *See, e.g.,*

¹ DHS argues that the holding of *Blackwell v. F.B.I.*, 646 F.3d 37 (D.C. Cir. 2011) should be ignored because “the court was not presented with the question of whether the different clauses of Exemption 7(E) contain different requirements.” Def.’s Reply and Opp., Dkt. 13, at 16. But the *Blackwell* court’s implicit holding echoes the approach to Exemption 7(E) taken by many courts in this circuit, even several that have adopted the “categorical protection” formulation advanced by DHS. *See, e.g., McRae v. U.S. Dep't of Justice*, 869 F. Supp. 2d 151, 168-69 (D.D.C. 2012) (adopting the “categorical protection” standard but evaluating whether disclosure would interfere with effectiveness); *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 . . .”); *Williams v. DOJ*, No. 02-2452, slip op.at11-12 (D.D.C. Feb. 4, 2004) (protecting “serial numbers on bait money” because “disclosure of this technique would undercut its usefulness”).

U.S. News, 1986 U.S. Dist. LEXIS 27634, at *8 (disclosing general pricing information related to armored limousines because without vehicle specifications such information enables “little more than speculation” as to the protection devices employed in a particular vehicle); *Pub. Employees for Env'tl. 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”). Thus, the shutdown questions should be 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.

Dated: August 23, 2013

Respectfully submitted,

/s/ Marc Rotenberg
MARC ROTENBERG
President and Executive Director
(D.C. Bar # 422825)

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

Attorneys for Plaintiff

¹-Admitted to practice in New York, admission pending in D.C.

²-Admitted to practice in Maryland, admission pending in D.C.