[ORAL ARGUMENT NOT YET SCHEDULED]
No. 14-5013

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

ELECTRONIC PRIVACY INFORMATION CENTER,

Plaintiff-Appellee,

v.

UNITED STATES DEPARTMENT OF HOMELAND SECURITY,

Defendant-Appellant.

On Appeal from the United States District Court for the District of Columbia

REPLY BRIEF

STUART F. DELERY
Assistant Attorney General

RONALD C. MACHEN, JR.
United States Attorney

SHARON SWINGLE
ADAM C. JED
(202) 514-8280
Attorneys, Appellate Staff
Civil Division, Room 7240
U.S. Department of Justice
950 Pennsylvania Ave., N.W.
Washington, DC 20530

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

A. Parties and Amici

The plaintiff-appellee is the Electronic Privacy Information Center. The defendant-appellant is the United States Department of Homeland Security.

B. Rulings Under Review

The defendant-appellant seeks review of the November 12, 2013 judgment and decision, issued by the Honorable James E. Boasberg, United States District Court for the District of Columbia, in Case No. 13-cv-260, ECF Nos. 18, 19. The district court's order and opinion are reproduced in the Joint Appendix at JA41 and JA42 respectively. No citation is yet available in the Federal Supplement. The district court's opinion can be found at 2013 WL 5976973.

C. Related Cases

This case has not previously been before this or any other court. We are not aware of any related cases.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Cases: **Page**

*Authorities upon which we chiefly rely are marked with asterisks.

Statutes:

Legislative Materials:

Other Authorities:

GLOSSARY

DHS	Department of Homeland Security
EPIC	Electronic Privacy Information Center
FOIA	Freedom of Information Act
JA	Joint Appendix
SOP 303	Department of Homeland Security Standard Operating Procedure 303

INTRODUCTION AND SUMMARY OF ARGUMENT

We showed in the opening brief that the district court erred in ordering disclosure of Standard Operating Procedure 303 ("SOP 303"), which contains highly sensitive procedures for the shutdown and restoration of wireless networks during critical emergencies such as the threatened use of remotely detonated explosives. SOP 303 comes within the plain language of FOIA Exemption 7(F), because its disclosure "could reasonably be expected to endanger the life or physical safety of any individual," 5 U.S.C. § 552(b)(7)(F). Making SOP 303 public could enable malefactors to plan around or interfere with the government's procedures for deciding whether to shut down wireless networks during threats and for executing a shutdown. SOP 303 is also protected under FOIA Exemption 7(E), which protects records and information that "would disclose techniques and procedures for law enforcement investigations or prosecutions," 5 U.S.C. § 552(b)(7)(E). As EPIC does not dispute, SOP 303 is a series of steps for use in response to critical emergencies that will trigger law enforcement investigations. Choosing whether, when, and where to shut down a cellular network is a logical component of an ongoing investigation triggered by the threat, and SOP 303 serves investigative functions such as protecting evidence and first responders and minimizing interference with 911 calls.

EPIC argues that Exemption 7(F) requires an agency to identify the individuals at risk with specificity, but the text of the statute does not impose such a requirement, nor does the legislative history support that construct. EPIC accuses the government

of reading "any individual" out of the statute, but the requirement that release must pose a threat to "any individual" reflects Congress's intent to expand the statute from protecting only law enforcement personnel to protecting people generally. Exemption 7(F) is not inapplicable when disclosure of a document could create a specific and non-speculative risk to a large, rather than a small, group of people.

EPIC also challenges the applicability of Exemption 7(E), arguing that SOP 303 is used for coordination rather than for law enforcement investigation or prosecution. This ignores the realities that law enforcement investigations often involve multiple persons and agencies. EPIC appears to suggest that Exemption 7(E) applies only to records that disclose an investigatory technique, such as surveillance techniques or polygraph information. But as we showed in our opening brief, Congress specifically expanded the statute to reach beyond "investigative techniques and procedures" to encompass "techniques and procedures *for* law enforcement investigations or prosecutions." As a procedure that will be used during an ongoing investigation and that will shield evidence and law enforcement personnel and minimize disruption to police communications and 911 calls, SOP 303 clearly satisfies this requirement. EPIC also argues that the government's interpretation leaves Exemption 7(A), which shields records that "could reasonably be expected to interfere with enforcement proceedings," as surplusage. However, a document or piece of information that is itself evidence, but does not describe "techniques or procedures," will typically be protected by Exemption 7(A), yet not Exemption 7(E).

Unable to find any support for the district court's interpretation of Exemptions 7(F) and (E), EPIC now contends that, even if some information in SOP 303 could be withheld, DHS failed to segregate non-exempt material. EPIC offers no basis to second-guess DHS's expert judgments about the risks of disclosing procedures for responding to critical emergencies like the threat of wireless-activated explosives. In any event, the issue is properly addressed by the district court in the first instance, under a correct construction of Exemptions 7(F) and 7(E).

ARGUMENT

A. The Department of Homeland Security Properly Withheld SOP 303 Under FOIA Exemption 7(F).

As our opening brief explained (at 11-18), the district court erred in construing Exemption 7(F)'s protection for information that "could reasonably be expected to endanger the life or physical safety of any individual" to apply only where the individual at risk is "identif[ied]" with "specificity." The text of Exemption 7(F) contains no requirement that there be an identifiable individual. Indeed, this is in contrast to provisions in FOIA's companion statute, the Privacy Act. See, *e.g.*, 5 U.S.C. § 552a(j)(2)(B). It is also implausible that Congress intended to permit an agency to withhold a document if disclosure poses a danger to a small group of specifically identifiable people, but to require disclosure if the danger posed is to many or most people.

EPIC quotes extensively from the district court decision and the Second Circuit's now-vacated decision in *ACLU* v. *Dep't of Defense*, 543 F.3d 59, 66-72 (2d Cir. 2008), *vacated on other grounds*, 558 U.S. 1042 (2009), but ignores much of the government's brief, which shows the flaws in those courts' reasoning. Thus, EPIC points (Br. 18-20) to the same snippets of legislative history relied on by the district court. As we have explained (at 17), even taken in isolation, those quotes do not support EPIC's rule that Exemption 7(F) applies only when release could endanger the life or physical safety of specifically identified individuals. And as we have further explained (at 17-18), those quotes are taken out of context. For example, the Deputy Attorney General's testimony that "[t]he provisions of Exemption 7 would be modified slightly" was part of a general observation that the proposed bill would "not revise[] wholesale" the existing Exemption 7, and she then referred to several amendments unrelated to the language in dispute between the parties here. 131 Cong. Rec. 248 (1985). Moreover, even EPIC understands this legislative history to show that the 1986 amendment replacing "law enforcement personnel" with "any person" was intended "only to relax the category of covered persons." EPIC Br. 19 (internal quotation marks omitted). And EPIC does not appear to dispute that prior to the amendment, Exemption 7(F) did not require the government to identify particular at-risk officials. See, *e.g., LaRouche* v. *Webster*, No. 75-cv-6010, 1984 WL 1061, at *8 (S.D.N.Y. Oct. 23, 1984) (applying Exemption 7(F) to block public disclosure of an

FBI report describing a home-made machine gun, in order to protect "law enforcement personnel" generally).

EPIC appears to derive (Br. 11-14) its atextual requirement of a specifically described individual from the required "nexus between disclosure and possible harm," *i.e.*, the requirement that disclosure "could *reasonably be expected to endanger* the life or physical safety of any individual," 5 U.S.C. § 552(b)(7)(F) (emphasis added). But EPIC does not explain why the release of records or information "could *reasonably be expected to endanger* the life or physical safety of any individual" only in circumstances where the threatened individual or individuals can be identified with specificity. EPIC's insistence that it "is not sufficient" to identify "people near unexploded bombs, people who frequent high value targets, and bomb squads and other first responders" (Br. 13) demonstrates both the lack of any logical basis for this rule, and the practical difficulty with its argument. Indeed, although EPIC appears to concede that its prophylactic rule would be satisfied for procedures concerning threats to small geographic areas, such as an inundation maps for single dams, EPIC does not explain why, for a procedure applicable to crises nationwide, there is not a nexus between disclosure and possible harm. The fact that release of records poses a concrete and non-speculative danger to a large group of people does not undermine the "nexus between disclosure and possible harm"; it underscores the fact that release "could reasonably be expected to endanger the life or physical safety of any individual."

EPIC's only textual defense of this rule is its argument (Br. 16-17) that, unless "any individual" in Exemption 7(F) is construed to mean "any individual identified with reasonable specificity," the phrase "any individual" will be "surplusage." Of course EPIC's own interpretation is at odds with the textual canon that Congress is understood to mean what it says. Moreover, the reference to "any individual" specifies *whose* life or physical safety must be at risk. It clarifies, for example, that Exemption 7(F) does not shield the life of animals or the physical safety of property. And more importantly, the phrase clarifies that Exemption 7(F) shields the life or physical safety of "any individual" rather than only the "law enforcement personnel" protected under the prior version. EPIC's argument is therefore merely a claim that perhaps Congress could have been clearer in specifying that the government *does not* have to identify the individuals at risk with specificity. "[T]he mere possibility of clearer phrasing cannot defeat the most natural reading of a statute." *Caraco Pharm. Labs., Ltd.* v. *Novo Nordisk A/S*, 132 S. Ct. 1670, 1682 (2012).

EPIC also contends (Br. 19-20) that if there is a real danger, DHS should classify the documents. The possibility of classification is neither coextensive nor mutually exclusive with Exemption 7(F) and, more importantly, it does not provide any reason for adopting EPIC's atextual rule. The fact that SOP 303 must be shared with federal law enforcement officials, state homeland security officials, and national cellular carriers creates practical barriers to classifying the document. The fact that the

document is not classified does not alter the conclusion that release of the procedures contained in SOP 303 could endanger the life and physical safety of many individuals.

Finally, and as we have explained (at 19-21), even if Exemption 7(F) applies only to a particularized threat to a discrete population, that requirement is satisfied here. Although the set of people who could be harmed as a result of disclosure of SOP 303 is large, there are identifiable groups who are more likely to be put at risk. These include people near unexploded bombs, people who frequent high-value targets, and members of bomb squads and other first responders. EPIC's only response is the assertion that this is "not sufficient to satisfy the 7(F) standard." Br. 13. This *ipse dixit* does not explain *why*, even if the government were required to show a particularized threat to a discrete population, the government has not done so here. To the extent that EPIC suggests (Br. 13-14) that Exemption 7(F) applies only when disclosure would reveal the at-risk individuals' "participation in law enforcement activities," that rule is also unsupported by the text and legislative history and is flatly inconsistent with *Pub. Emps. for Envtl. Responsibility* v. *U.S. Section, Int'l Bound. & Water Comm'n, U.S.-Mexico ("PEER")*, 740 F.3d 195 (D.C. Cir. 2014), which applied Exemption 7(F) to protect individuals living downstream from dams. *Id.* at 199, 206.

B. The Department of Homeland Security Properly Withheld SOP 303 Under FOIA Exemption 7(E).

Exemption 7(E) protects records or information that, as relevant here, "would disclose techniques and procedures for law enforcement investigations or

prosecutions," 5 U.S.C. § 552(b)(7)(E). As our opening brief explained (at 21-24), this statutory language reflects an intentional choice to shield not only investigative techniques and procedures but also *non*-investigative techniques or procedures, so long as they are for law enforcement investigations or prosecutions.

At places in its brief, EPIC appears to construe Exemption 7(E) as limited to "the process of an inquiry, such as methods of gathering or organizing information." Br. 22-23. That position, however, mistakenly applies the pre-1986 requirement that production would disclose "*investigative* techniques and procedures," 5 U.S.C. § 552(b)(7)(E) (1982) (emphasis added), rather than the present requirement that production would disclose "techniques and procedures *for* law enforcement investigations," 5 U.S.C. § 552(b)(7)(E) (emphasis added). "When Congress acts to amend a statute," courts "presume it intends its amendment to have real and substantial effect." *Stone* v. *INS*, 514 U.S. 386, 397 (1995). And here, the legislative history confirms that the textual change was meant to accomplish exactly what the text indicates, "to make clear that 'techniques and procedures for law enforcement investigations and prosecutions' can be protected, regardless of whether they are 'investigative' or non-investigative." S. Rep. No. 98-221, at 24 (1983) ("Senate Report").

Elsewhere, EPIC appears to concede (*e.g.,* Br. 25) that Exemption 7(E) encompasses more than solely investigative techniques, but does not explain why procedures for preventing remote detonation of bombs while minimizing disruption

to wireless communications such as 911 calls do not constitute techniques or procedures "for law enforcement investigations," 5 U.S.C. § 552(b)(7)(E). EPIC does not dispute that the procedures in SOP 303 apply only when there is a serious threat that will trigger a law enforcement investigation. Choosing whether, when, and where to shut down a cellular network is a logical component of an ongoing investigation triggered by the threat. EPIC also does not appear to dispute that the procedures in SOP 303 directly support such investigations and, indeed, serve investigative functions. Procedures for stopping detonation of bombs not only save innocent lives but also protect first responders investigating the events and witnesses who can offer helpful clues, and preserve valuable physical evidence such as undetonated bombs. These procedures also ensure that first responders such as police bomb squads and arson units can quickly and effectively deploy, and that the public can make wireless calls, including 911 calls.

EPIC appears to urge (Br. 20-21, 26) that the procedures in SOP 303 cannot be "for law enforcement investigations" because they are used to "coordinate" other entities. This argument misses the mark. The steps in SOP 303 are used by federal and state law enforcement agencies and cellular companies to decide whether, when, where, and how to shut down and restore wireless communications during critical emergencies and to execute those decisions. See JA 16-18. And those procedures, in turn, directly support enforcement investigations that may be run by state and/or federal agencies. EPIC's argument ignores the reality that law enforcement often

involves multiple persons and agencies. Techniques or procedures may be "for law enforcement investigations," 5 U.S.C. § 552(b)(7)(E), even if used by multiple entities, or created by one entity for another's use.

EPIC posits that the government's interpretation of Exemption 7(E)'s protection for "techniques and procedures for law enforcement investigations" is "boundless." Br. 23. But Exemption 7(E) is bounded by the statutory language: it applies to "records or information compiled for law enforcement purposes," and even then, only when disclosure of such records or information would reveal "techniques and procedures for law enforcement investigations." 5 U.S.C. § 552(b)(7)(E). This is not a case where "technique[s] might indirectly create conditions conducive to a future investigation." EPIC Br. 23. Rather, as EPIC has not disputed, it is a case where techniques and procedures directly aid in an ongoing investigation. EPIC's assertion that FOIA exemptions should be read narrowly (*ibid.*), must be balanced against Congress's clear intent that FOIA's exemptions be given "meaningful reach and application" in order to protect "legitimate governmental and private interests [that] could be harmed by release of certain types of information." *John Doe Agency* v. *John Doe Corp.*, 493 U.S. 146, 152 (1989) (internal quotation marks omitted); see also *CIA* v. *Sims*, 471 U.S. 159, 166-167 (1985); *FBI* v. *Abramson*, 456 U.S. 615, 630-631 (1982); *Weinberger* v. *Catholic Action*, 454 U.S. 139, 144 -145(1981); *Ctr. for Nat'l Sec. Studies* v. *DOJ*, 331 F.3d 918, 925 (D.C. Cir. 2003).

Finally, EPIC argues that the government's interpretation of Exemption 7(E) would "render[] other FOIA exemptions superfluous," such as Exemption 7(A)'s protection of records that "could reasonably be expected to interfere with enforcement proceedings." Br. 25 (quoting 5 U.S.C. § 552(b)(7)(A)). Of course, statutes often contain overlapping protections meant to ensure that there are no critical gaps. That approach makes particular sense when dealing with sensitive law enforcement records. In any event, although there may be some overlap, Exemption 7(E) does not render Exemption 7(A) superfluous. Release of a record that *does not* contain "techniques and procedures," for example, such as a document identifying confidential sources, nonetheless may "reasonably be expected to interfere with enforcement proceedings," 5 U.S.C. § 552(b)(7)(A); see, *e.g., NLRB* v. *Robbins Tire & Rubber Co.*, 437 U.S. 214, 236-242 (1978) (witness statements that would reveal identity of sources, thus allowing witness intimidation and deterring cooperation); *Juarez* v. *DOJ*, 518 F.3d 54, 58-59 (D.C. Cir. 2008) (DEA records identifying confidential source and enabling destruction of evidence).

C. The Department of Homeland Security Properly Considered Segregability.

Unable to find any support for the district court's interpretations of Exemptions 7, EPIC now contends (Br. 27-31) that DHS failed properly to segregate non-exempt material under 5 U.S.C. § 552(b).

The district court did not address this issue, because it held that Exemptions 7(E) and 7(F) are wholly inapplicable. Therefore, this Court need not reach the issue, which can instead be addressed in the first instance by the district court under the correct interpretation of Exemptions 7(E) and 7(F). If this Court reaches the issue, however, DHS has adequately established that it withheld exempt information in SOP 303 and disclosed reasonably segregable portions of the document to EPIC.

"[A]gencies are entitled to a presumption that they complied with their obligation to disclose any reasonably segregable portion of a record." *Boyd* v. *Crim. Div. of the U.S. DOJ,* 475 F.3d 381, 391 (D.C. Cir. 2007). An agency can justify its withholdings by providing a description of the withheld material, in conjunction with a declaration establishing that the agency has reviewed the document and determined that no other information may be released without compromising the withheld material. See *Johnson* v. *Exec. Office for U.S. Att'ys.*, 310 F.3d 771, 776 (D.C. Cir. 2002); *Armstrong* v. *Exec. Office of the President*, 97 F.3d 575, 578-580 (D.C. Cir. 1996).

Here, DHS conducted a segregability review of SOP 303 (JA 17) and disclosed portions of the document, including the statement of purpose and list of state homeland security offices (with privacy redactions not challenged by EPIC) that would be involved in the process of deciding whether to shut down a wireless network. See SA 1-30. A DHS official explained in a sworn declaration that SOP 303 includes "the pre-determined series of questions that determines if a shutdown is necessary, and the executing protocols related to the implementation of SOP 303,"

that DHS conducted "a review for segregability," and that "[p]ortions of the SOP are being withheld," as relevant here, pursuant to Exemptions 7(E) and 7(F), because they "contain[] security procedures and related information regarding the shutdown of cell phone service during various types of homeland security incidents." JA 17; see JA 18-19 (expanding on the application of Exemption 7(E) and 7(F) to these procedures). Thus, DHS explained that SOP 303 includes a "protocol for verifying that circumstances exist that would justify shutting down wireless networks" and considering "the inability of first-responders and the public to use wireless phones for calls, including 911 calls" and that SOP 303 includes "a step-by-step process" for then shutting down and restoring wireless networks. JA 18. DHS further explained that disclosure of these procedures "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." JA 18-19; accord JA 19. This explanation adequately supports withholding of the relevant portions of SOP 303, and EPIC cannot overcome the applicable presumption of good faith simply by observing (Br. 28-29) that DHS redacted much of the part of SOP 303 containing substantive procedures.

EPIC also contends (Br. 29-30) that, even if portions of SOP 303 were properly withheld, the "predetermined shutdown questions contained within SOP 303" must be disclosed because they "are plainly not law enforcement techniques."

As an initial matter, EPIC's argument about "law enforcement techniques" implicates only Exemption 7(E), not Exemption 7(F), which also provides a basis for withholding the redacted procedures. But EPIC's argument also fails under Exemption 7(E), because it rests on an unsupportable distinction between the questions that determine if a shutdown is necessary, and the "procedures" or "techniques" for making that determination. The "pre-determined series of questions that determines if a shutdown is necessary" (JA 17) is a series of steps for determining whether "circumstances exist that would justify shutting down wireless networks," and considering effects "such as the inability of first-responders and the public to use wireless phones for calls, including 911 calls." JA 18; *see Webster's Third New International Dictionary* 1807 (1993) (defining "procedure" as "a particular way of doing or going about the accomplishment of something"). A series of questions that must be considered to determine if a shutdown should occur is also a technique for making that decision and thus for preventing remote activation of explosives and balancing other effects of a shutdown. See *id.* at 2348 (defining "technique" as "a technical method of accomplishing a desired aim").

EPIC also argues (Br. 30) that the government has not made an adequate showing of harm by demonstrating that "disclosure would allow bad actors to evade, defeat, or otherwise circumvent" techniques or procedures for law enforcement investigations. EPIC's argument, however, rests on a portion of Exemption 7(E) that protects information the disclosure of which "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). The government did not rely on that portion of Exemption 7(E), instead invoking an earlier part of Exemption 7(E) that shields records that "would disclose techniques and procedures for law enforcement investigations or prosecutions," 5 U.S.C. § 552(b)(7)(E).

To the extent that EPIC asserts that disclosure of techniques and procedures must also be reasonably expected to risk circumvention of the law, this misunderstands the text. Under the "rule of the last antecedent," a "limiting clause or phrase" ordinarily should "be read as modifying only the noun or phrase that it immediately follows." *Barnhart* v. *Thomas,* 540 U.S. 20, 26 (2003). Thus, the condition in the second clause in Exemption 7(E) that "disclosure could reasonably be expected to risk circumvention of the law" applies only to disclosure of "guidelines for law enforcement investigations or prosecutions." The sentence structure confirms this conclusion. Exemption 7(E) applies when disclosure "*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) (emphases added). By separating the two clauses in Exemption 7(E) with a single comma and the disjunctive "or," and by repeating the phrase "would disclose" at the beginning of each clause, Congress made clear the stand-alone character of each clause and that the circumvention standard applies only to the second clause. See also

Allard K. Lowenstein Int'l Human Rights Project v. *DHS*, 626 F.3d 678, 681-682 (2d Cir. 2010).

If there were any doubt, the drafting history further confirms this conclusion. The second clause in Exemption 7(E)—exempting records or information that "would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law"—was added by Congress later in time as a single unit "to address some confusion created by . . . *Jordan* v. *U.S. Dept. of Justice*, 591 F.2d 753 (D.C. Cir. 1978)." Senate Report 25; see U.S. Dep't of Justice, *Attorney General's Memorandum on the 1986 Amendments to the Freedom of Information Act* 16 (1987) (describing "Exemption 7(E)'s entirely new second clause" as a "distinct new provision" that overrules *Jordan*); *id.* at 16 n.27 (confirming that the "first clause of Exemption 7(E)"— the "'technique and procedure' protection" —"is such that it does not require any particular determination of 'harm'"). Like the text, the drafting history thus shows that the two clauses are distinct and that the circumvention standard in the second clause is inapplicable to the first.[1]

[1] In *Blackwell* v. *FBI*, 646 F.3d 37 (D.C. Cir. 2011), this Court analyzed the possibility of circumvention for records containing techniques and procedures. See *id.* at 41-42; cf. *PEER*, 740 F.3d at 204 n.4. But the Court did not address whether the circumvention requirement modifies both phrases in Exemption 7(E). See *Blackwell*, 646 F.3d at 41-42. That is so because the issue was not presented. The parties discussed together the "risk circumvention" requirements of the now-abrogated "high 2" exemption and Exemption 7(E) and argued primarily about whether there was a

Continued on next page.

Moreover, even if a "risk circumvention" requirement applied, it would be easily met. See *PEER,* 740 F.3d at 205 (holding that requirement sets a "low bar"); *Mayer Brown LLP* v. *IRS*, 562 F.3d 1190, 1193 (D.C. Cir. 2009) (explaining the standard). If a bad actor had "information about when shutdown procedures are used and how a shutdown is executed," he could "circumvent or interfere" with that strategy. JA 18-19. EPIC posits that the list of pre-determined questions would not be sufficient in itself "for 'bad actors to insert themselves into the process of shutting down or reactivating wireless networks.'" Br. 31 (quoting JA 19). Directly inserting oneself into a shutdown or restoration, however, is only one example offered by DHS of the ways that the withheld material could be used to circumvent or interfere with this procedure for preventing the triggering of explosive devices. See JA 19 (disclosure "would, *e.g.*, enable bad actors to insert themselves into the process"). Moreover, there is no requirement that withheld information be sufficient in itself to allow circumvention, only that it could pose a reasonable risk of circumvention. See *Mayer Brown*, LLP, 562 F.2d at 1193. (Likewise, if EPIC intends to challenge the

---

risk of circumvention. See Brief for Appellant, 2010 WL 6368289, at *37-40, No. 10-5072; Brief of Appellee, 2010 WL 6368288, at *30-36; Reply Brief, 2011 WL 2446101, at *29-32. Indeed, the appellant's description of the applicable standard for Exemption 7(E) appeared to contemplate that the circumvention requirement applies only to guidelines and not to procedures or techniques. See Brief for Appellant, 2010 WL 6368289, at *39 ("[F]or Exemption 7(E) to apply, the information in question must either (1) reveal a law enforcement technique that is generally unknown to the public, or (2) disclose law enforcement guidelines that could reasonabl[y] be expected to risk circumvention of the law.").

applicability of Exemption 7(F), the question is whether release "*could reasonably be expected* to endanger.") DHS reasonably concluded that disclosure about "when shutdown procedures are used and how a shutdown is executed" would allow a bad actor to "circumvent or interfere" with the government's method of addressing these critical threats. JA 18-19.

If the Court believes that this issue requires further consideration, however, the matter should be remanded to the district court to consider in the first instance.

CONCLUSION

The judgment of the district court should be reversed.

Respectfully submitted,

STUART F. DELERY
Assistant Attorney General

RONALD C. MACHEN, JR.
United States Attorney

SHARON SWINGLE
/s/ Adam Jed
ADAM C. JED
(202) 514-8280
Attorneys, Appellate Staff
Civil Division, Room 7240
U.S. Department of Justice
950 Pennsylvania Ave., N.W.
Washington, DC 20530

AUGUST 2014

CERTIFICATE OF COMPLIANCE WITH FEDERAL RULE OF APPELLATE PROCEDURE 32(a)

I hereby certify that this brief complies with the requirements of Fed. R. App. P. 32(a)(5) and (6) because it has been prepared in 14-point Garamond, a proportionally spaced font. I further certify that this brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because it contains 4,386 words, excluding the parts of the brief exempted under Rule 32(a)(7)(B)(iii), according to the count of Microsoft Word.

/s/ Adam Jed

Adam C. Jed

CERTIFICATE OF SERVICE

I hereby certify that on August 4, 2014, I electronically filed the foregoing brief with the Clerk of the Court for the United States Court of Appeals for the District of Columbia Circuit by using the appellate CM/ECF system.

/s/ Adam Jed

Adam C. Jed