

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

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

**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.)	Civil Action No. 13-00260 (JEB)
)	
U.S. DEPARTMENT OF)	
HOMELAND SECURITY)	
)	
Defendant.)	
_____)	

**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 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 record 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. Env'tl. 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.



Homeland
Security

October 25, 2012

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

Re: **DHS Appeal Number 2013-HQAP-00004**
FOIA Request Number DHS/OS/PRIV 12-0598

Dear Ms. Stepanovich:

The Department of Homeland Security (DHS) has received your appeal of the response by the Privacy Office to your Freedom of Information Act (FOIA) request concerning Standard Operating Procedure 303. On behalf of the Deputy Associate General Counsel for General Law, we acknowledge your appeal and are assigning it number **2013-HQAP-00004** for tracking purposes. Please reference this number in any future communications about your appeal.

A high number of FOIA requests have been received by the Department. Accordingly, we have adopted the court-sanctioned practice of generally handling backlogged appeals on a first-in, first-out basis.¹ While we will make every effort to process your appeal on a timely basis, there may be some delay in resolving this matter. Should you have any questions concerning the processing of your appeal, please contact me at james.holzer@hq.dhs.gov.

Sincerely,

A handwritten signature in black ink that reads "James V. Holzer, Jr." with a stylized flourish at the end.

James Holzer
Director
Disclosure and FOIA Operations

¹ Appeals of expedited treatment denials will be handled on an expedited basis.

September 25, 2009

FOR OFFICIAL USE ONLY

NCC SOP 303

Warning: This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official. State and local Homeland security officials may share this document with authorized security personnel without further approval from DHS.



NCC STANDARD OPERATING PROCEDURE (SOP) 303:

Emergency Wireless Protocols

1. Purpose. This SOP provides detailed procedures for the National Coordinating Center for Telecommunications (NCC) to coordinate requests for the disruption of cellular service.

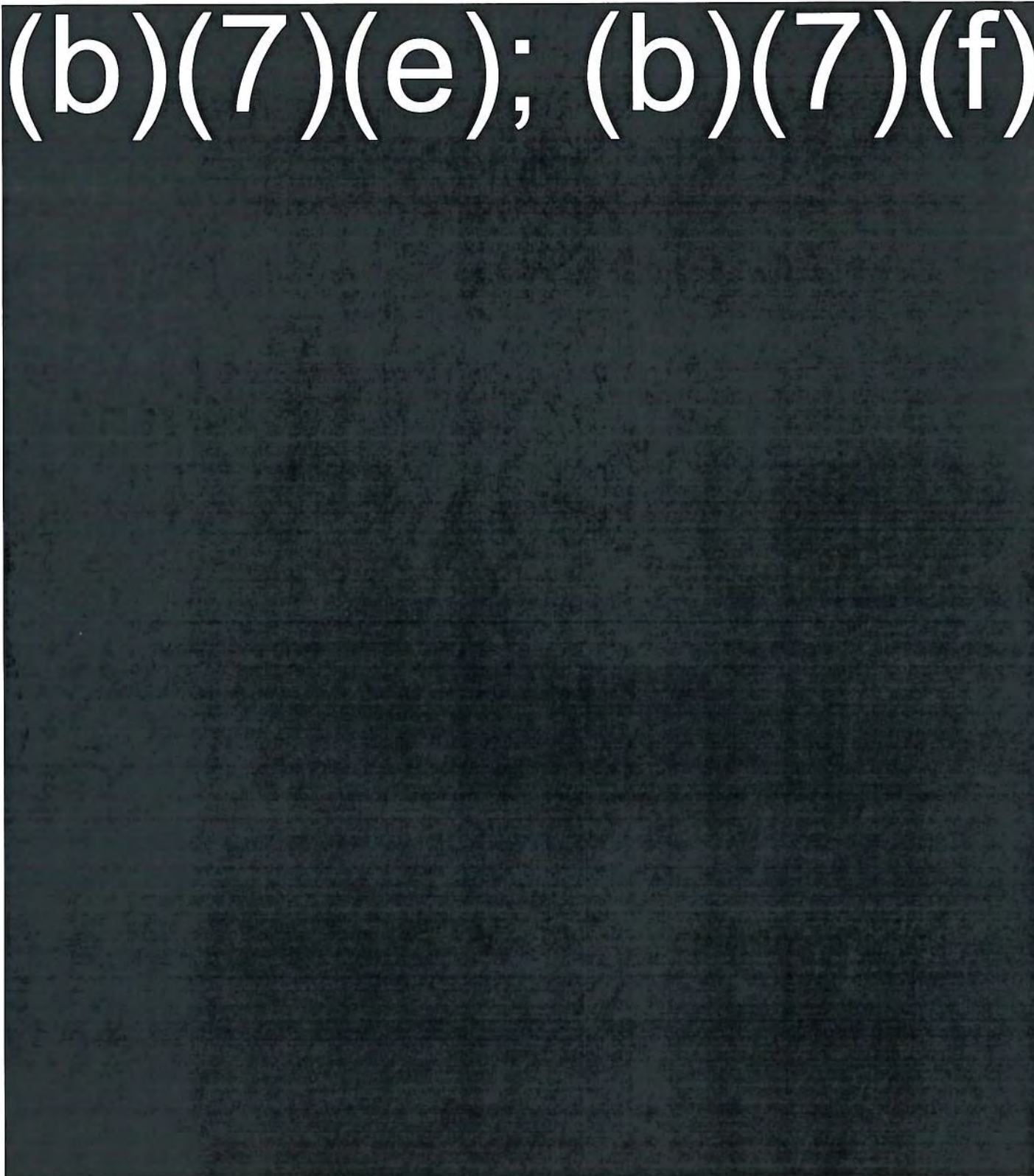
(b)(7)(e); (b)(7)(f)

September 25, 2009

FOR OFFICIAL USE ONLY

NCC SOP 303

(b)(7)(e); (b)(7)(f)



September 25, 2009

FOR OFFICIAL USE ONLY

NCC SOP 303

(b)(7)(e); (b)(7)(f)

5. Fax Confirmation. (b)(7)(e); (b)(7)(f)

This fax transmission will be scanned to a file for electronic distribution upon receipt.

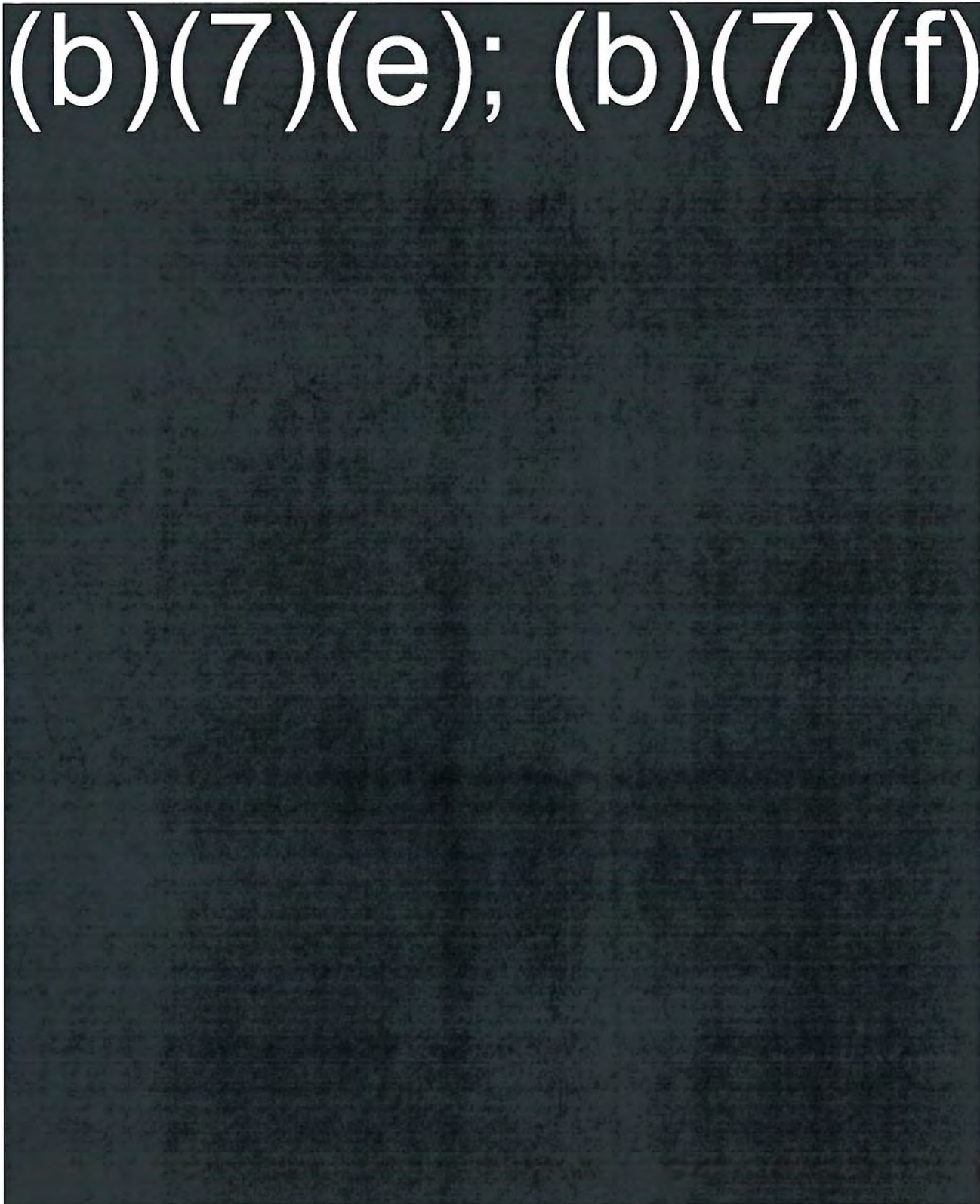
(b)(7)(e); (b)(7)(f)

September 25, 2009

FOR OFFICIAL USE ONLY

NCC SOP 303

(b)(7)(e); (b)(7)(f)

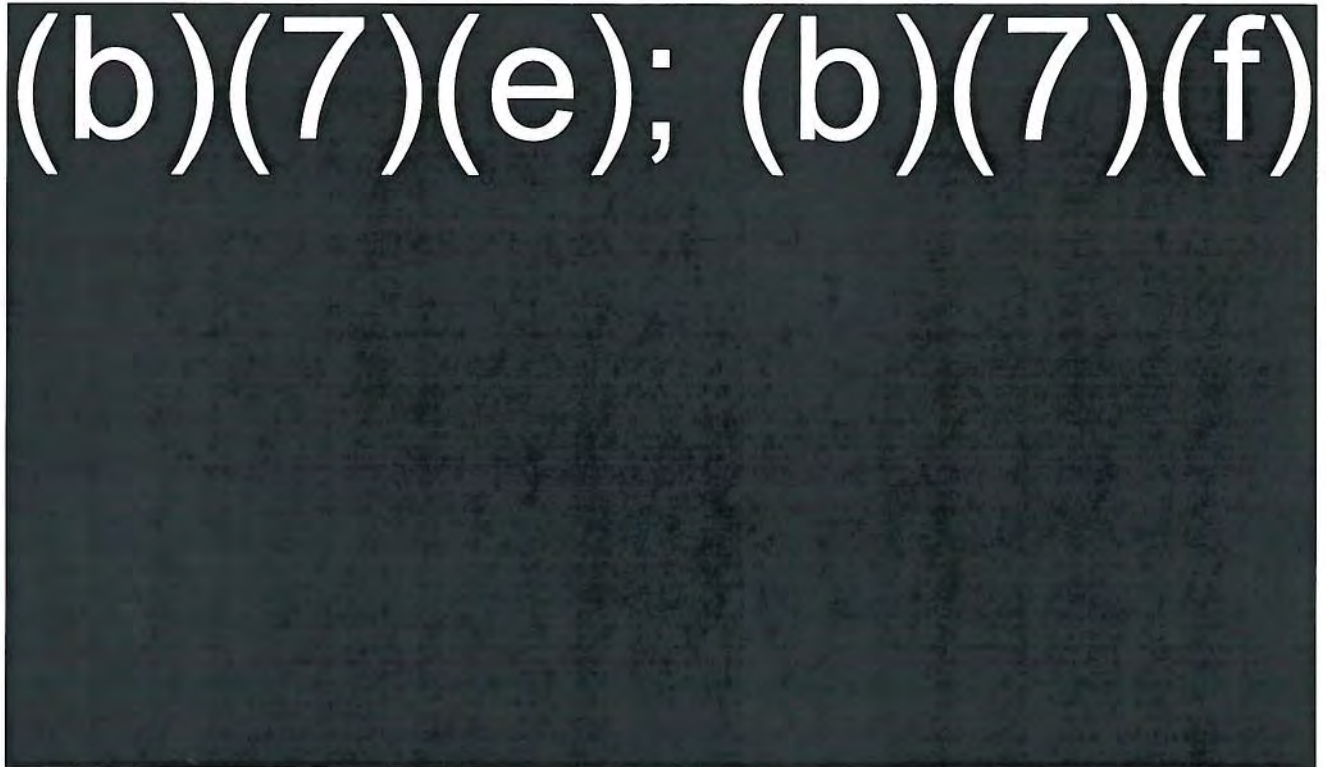


September 25, 2009

FOR OFFICIAL USE ONLY

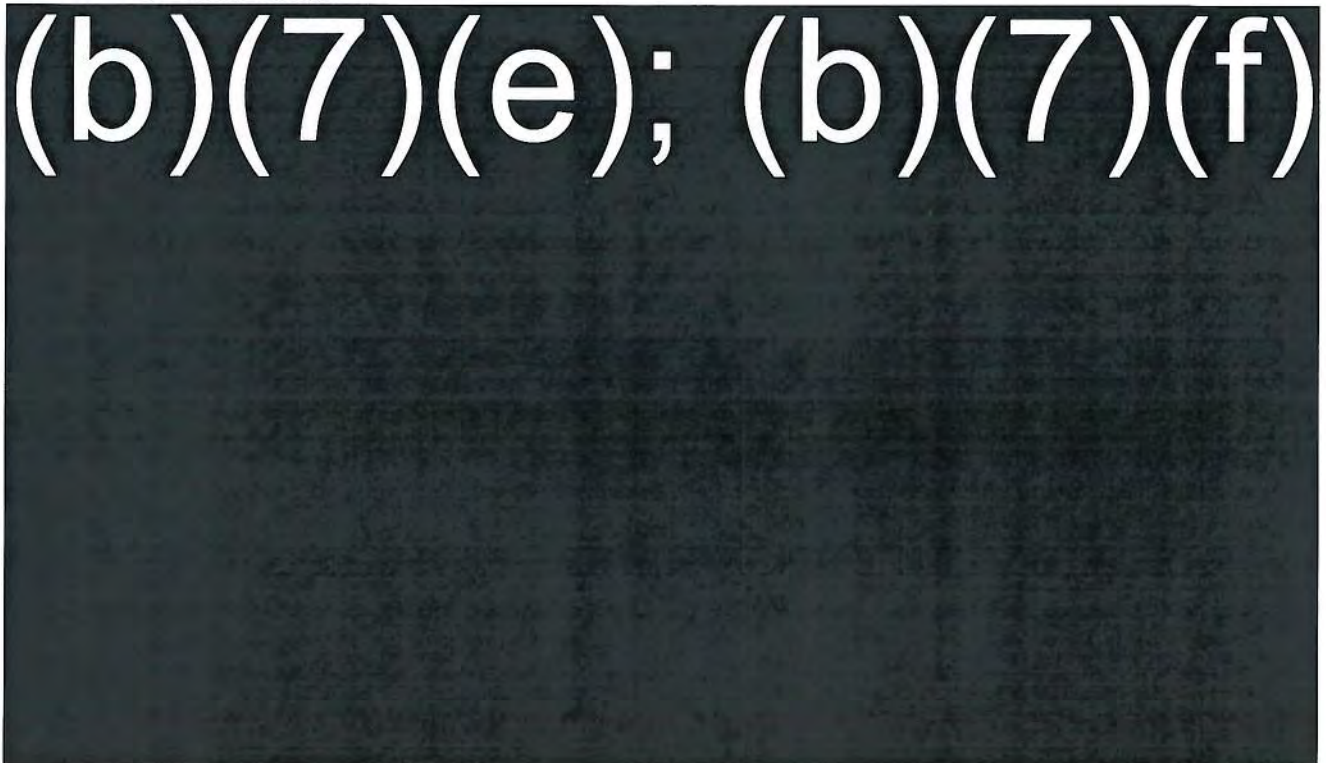
NCC SOP 303

(b)(7)(e); (b)(7)(f)



b. Restoration

(b)(7)(e); (b)(7)(f)



September 25, 2009

FOR OFFICIAL USE ONLY

NCC SOP 303

(b)(7)(e); (b)(7)(f)

ii. Notification

(b)(7)(e); (b)(7)(f)

September 25, 2009

FOR OFFICIAL USE ONLY

NCC SOP 303

(b)(7)(e); (b)(7)(f)

(b)(7)(e); (b)(7)(f)

6. Review. Review annually and following any instance where these procedures are implemented.
7. Supersession. This is the initial issue of this SOP.

September 25, 2009

FOR OFFICIAL USE ONLY

NCC SOP 303

Appendix A: Points of Contact

Appendix A will be updated as required based on input provided by the State Homeland Security Advisors.

ALABAMA

Alabama Emergency Management Agency
5898 County Road 41, P.O. Drawer 2160, Clanton, Alabama 35046-2160
Ph: 251/280-2200
Fax: 205/280-2493
24-Hr: 800/843-0699

(b)(6); (b)(7)(c)
(b)(6); (b)(7)(c)
(b)(6); (b)(7)(c)

ALASKA

Alaska Div. of Homeland Security and Emergency Management
P.O. Box 5750, Fort Richardson, AK 99505-5750
Ph: 602/244-0504
Fax: 907/428-7009
24-Hr: 907/428-7000

(b)(6); (b)(7)(c)
(b)(6); (b)(7)(c) (b)(6); (b)(7)(c)
(b)(6); (b)(7)(c)

ARIZONA

Arizona Div. of Emergency Management
5636 E. McDowell Road, Phoenix, AZ 85008-3495
Fax: 602/231-6263
24-Hr: 800/411-2336

(b)(6); (b)(7)(c)

ARKANSAS

Arkansas Department of Emergency Management
P.O. Box 758, Conway, AR 72033
Ph: 501/730-9750 (24-Hr.)
Fax: 501/730-9778
Emergency: 800/322-4012 or 501/730-9751

(b)(6); (b)(7)(c)

CALIFORNIA

California Office of Emergency Services
3650 Schriever Avenue, Mather, CA 95655
Ph: 916/845-8510
Fax: 916/845-8506

(b)(6); (b)(7)(c)

September 25, 2009

FOR OFFICIAL USE ONLY

NCC SOP 303

(b)(6); (b)(7)(c)

COLORADO

Division of Emergency Management
9195 East Mineral Avenue, Suite 200, Centennial, Colorado 80112
Ph: 720/852-6600
Fax: 720/852-6750

(b)(6); (b)(7)(c)

CONNECTICUT

Department of Emergency Management and Homeland Security
25 Sigourney Street, 6th Floor, Hartford, CT 06106-5042
Ph: 860/256-0800 or 800/397-8876
Fax: 860/256-0815

(b)(6); (b)(7)(c)

DELAWARE

Department of Safety and Homeland Security
Delaware Emergency Management Agency
165 Brick Store Landing Road, Smyrna, DE 19977
Ph: 302/659-3362
Fax: 302/659-6855
24-Hr: 877/729-3362 (Delaware Only)

(b)(6); (b)(7)(c)
(b)(6); (b)(7)(c)

DISTRICT OF COLUMBIA

(b)(6); (b)(7)(c)
(b)(6); (b)(7)(c)
Homeland Security & Emergency Management Agency
2720 Martin Luther King Jr. Ave., SE.
Washington, DC 20032
Fax: 202/673-7054 or 202/673-2290
24-Hr: 202/727-6161 (Shift Supervisor)

(b)(6); (b)(7)(c)

FLORIDA

Division of Emergency Management
2555 Shumard Oak Boulevard, Tallahassee, FL 32399-2100
24-Hr: 850/413-9911 and 800/320-0519
Fax: 850/488-1739

(b)(6); (b)(7)(c)

September 25, 2009

FOR OFFICIAL USE ONLY

NCC SOP 303

(b)(6); (b)(7)(c)

GEORGIA

Georgia Emergency Management Agency
935 East Confederate Avenue, SE, Atlanta, GA 30316
Ph: 404/ 635-7000 or 1-800-TRY-GEMA (in Georgia only)
Fax: 404/635-7205

(b)(6); (b)(7)(c)
(b)(6); (b)(7)(c)
(b)(6); (b)(7)(c)

HAWAII

Oahu Civil Defense Agency
650 S. King Street, Basement, Honolulu, HI 96813
Fax: 808/524-3439
24-Hr: 808/529-3911

(b)(6); (b)(7)(c)
Fax: 808/270-7275
24-Hr: 808/244-6400

(b)(6); (b)(7)(c)
Hawaii County Civil Defense Agency
920 Ululani Street, Hilo, HI 96720
Fax: 808/935-6460
24-Hr: 808/935-3311
(b)(6); (b)(7)(c)

IDAHO

Bureau of Homeland Security
4040 Guard Street, Bldg. 600, Boise, ID 83705-5004
Ph: 208/334-3460
Fax: 208/334-2322
24-Hr: 208/846-7610 or 800/632-8000 (Idaho only)

(b)(6); (b)(7)(c)

ILLINOIS

(b)(6); (b)(7)(c)
(b)(6); (b)(7)(c)

Illinois Emergency Management Agency
110 E. Adams Street, Springfield, IL 62701
Fax: 217/557-2145
24-Hr: 217/782-7860

(b)(6); (b)(7)(c)

September 25, 2009

FOR OFFICIAL USE ONLY

NCC SOP 303

INDIANA

State Emergency Management Agency
302 W. Washington, Room E-208, Indianapolis, IN 46204-2760
Ph: 317/232-3830
Fax: 317/232-3895
24-Hr: 800/669-7362

(b)(6); (b)(7)(c)
[Redacted]

IOWA

(b)(6); (b)(7)(c)
[Redacted]

Homeland Security and Emergency Management Division
Hoover State Office Building
1305 E. Walnut, Level A, Des Moines, IA 50319-0113
Fax: 515/281-7539
24-Hr: 515/281-3231

(b)(6); (b)(7)(c)
[Redacted]

KANSAS

Division of Emergency Management
2800 S.W. Topeka Blvd., Topeka, KS 66611-1287
Ph: 785/274-1409
Fax: 785/274-1426
24-Hr: 785/296-3176 or 800/905-7521

(b)(6); (b)(7)(c)
[Redacted]

KENTUCKY

Division of Emergency Management
Emergency Operations Center
100 Minuteman Parkway, Boone Center, Frankfort, KY 40601-6168
Ph: 502/607-1638
Fax: 502/607-1614
24-Hr: 800/255-2587

(b)(6); (b)(7)(c)
[Redacted]

LOUISIANA

Office of Homeland Security and Emergency Preparedness
7667 Independence Blvd., Baton Rouge, LA 70806
Ph: 225/925-7500
Fax: 225/925-7501

(b)(6); (b)(7)(c)
[Redacted]

September 25, 2009

FOR OFFICIAL USE ONLY

NCC SOP 303

(b)(6); (b)(7)(c)

MAINE

Maine Emergency Management Agency
72 State House Station, Augusta, ME 04333-0072
Ph: 207/624-4400
24-Hr: 207/624-7000 or 1-800-452-8735 (in-state only)

(b)(6); (b)(7)(c)

MARYLAND

Maryland Emergency Management Agency
5401 Rue St. Lo Drive, Reisterstown, MD 21136
Fax: 410/517-3610
24-Hr: 410/517-3600

(b)(6); (b)(7)(c)

MASSACHUSETTS

Emergency Management Agency
400 Worcester Road (Route 9 Eastbound), Framingham, MA 01702-5399
Ph: 508/820-2000
Fax: 508/820-2030
24-Hr: 508/820-2000

(b)(6); (b)(7)(c)

MICHIGAN

(b)(6); (b)(7)(c)

Emergency Management Division
P.O. Box 30636, Lansing, MI 48909-8136
Ph: 517/332-2521
Fax: 517/333-4987

(b)(6); (b)(7)(c)

MINNESOTA

Homeland Security and Emergency Management
444 Cedar Street, Suite 223, St. Paul, MN 55101-6223
Ph: 651-296-2233
Fax: 651/296-0459 or 651/297-7372

(b)(6); (b)(7)(c)

September 25, 2009

FOR OFFICIAL USE ONLY

NCC SOP 303

(b)(6); (b)(7)(c)

MISSISSIPPI

Mississippi Emergency Management Agency
1410 Riverside Drive, Jackson, MS 39202-1297
P.O Box 4501, Jackson, MS 39296-4501
Phone: 601/352-9100
Fax: 601/352-8314
24-Hr: 1-800-222-MEMA(6362)

(b)(6); (b)(7)(c)

MISSOURI

Emergency Management Agency
2302 Militia Drive, P.O. Box 116, Jefferson City, MO 65102
Fax: 573/526-9261
24-Hr: 573/751-2748

(b)(6); (b)(7)(c)

MONTANA

Disaster and Emergency Services
P.O. Box 4789 mitigation, Helena, MT 59604-4789
Ph: 406/841-3911 (duty officer)
Fax: 406/841-3965
Emergency: 406/841-3911

(b)(6); (b)(7)(c)

NEBRASKA

Emergency Management Agency
1300 Military Road, Lincoln, NE 68508-1090
Fax: 402/471-7433
24-Hr: 402/471-7421 and 877/297-2368

(b)(6); (b)(7)(c)

NEVADA

Department of Public Safety
Division of Emergency Management
2525 S. Carson Street, Carson City, NV 89711
Ph: 775/687-4240
Fax: 775/687-6788
24-Hr: 775/688-2830

(b)(6); (b)(7)(c)

September 25, 2009

FOR OFFICIAL USE ONLY

NCC SOP 303

NEW HAMPSHIRE

Division of Emergency Services, Communications and Emergency Management
Bureau of Emergency Management
33 Hazen Drive, Concord, NH 03305
107 Pleasant Street, State Office Park South, Concord, NH 03301
Fax: 603/225-7341
24-Hr: 603/271-3636 or 1-800-852-3792 (New Hampshire WATS line)

(b)(6); (b)(7)(c)

NEW JERSEY

Department of Environmental Protection State Emergency Response Commission (SERC)
New Jersey Office of Emergency Management
P.O. Box 7028, Trenton, NJ 08628
Fax: 609/777-0985

(b)(6); (b)(7)(c)

NEW MEXICO

New Mexico Department of Public Safety
Office of Emergency Management
PO Box 1628, Santa Fe, NM 87504
Fax: 505/476-9695
24-Hr: 505/476-9635

(b)(6); (b)(7)(c)

NEW YORK

State Emergency Management Office
1220 Washington Avenue, Building 22, Suite 101, Albany, NY 12226-2251
Ph: 518/292-2000
Fax: 518/457-9930
24-Hr: 518/457-2200

(b)(6); (b)(7)(c)

NORTH CAROLINA

(b)(6); (b)(7)(c)

Division of Emergency Management

September 25, 2009

FOR OFFICIAL USE ONLY

NCC SOP 303

116 W Jones St, Raleigh, NC 27603
Ph: 919/733-3867
Fax: 919/733-7554
24-Hr: 919/733-3300 or 800/858-0368

(b)(6); (b)(7)(c)

NORTH DAKOTA

Division of Emergency Management
P.O. Box 5511, Bismarck, ND 58506-5511
Ph: 701/328-8100
Fax: 701/328-8181
24-Hr: 701/328-9921

(b)(6); (b)(7)(c)

OHIO

(b)(6); (b)(7)(c)

Ohio Emergency Management Agency
2855 W. Dublin-Granville Road, Columbus, OH 43235-2206
Fax: 614/889-7183
24-Hr.: 614/889-7150

(b)(6); (b)(7)(c)

OKLAHOMA

Department of Emergency Management
2401 Lincoln Blvd - Suite C51, P.O. Box 53365, Oklahoma City, OK 73152
Ph: 405/521-2481
Fax: 405/521-4053
24-Hr: 800/800-2481

(b)(6); (b)(7)(c)

OREGON

(b)(6); (b)(7)(c)

Oregon Emergency Management
P.O. Box 14370, Salem, OR 97309-5062
Fax: 503/588-1378
24-Hr: 800/452-0311

(b)(6); (b)(7)(c)

September 25, 2009

FOR OFFICIAL USE ONLY

NCC SOP 303

PENNSYLVANIA

Pennsylvania Emergency Management Agency
2605 Interstate Drive , Harrisburg, PA 17110-9364
Fax: 717/651-2021
24-Hr: 717/651-2001

(b)(6); (b)(7)(c)
[Redacted]

RHODE ISLAND

Emergency Management Agency
645 New London Avenue, Cranston, RI 02920
Fax: 401/944-1891
24-Hr: 401/946-9996

(b)(6); (b)(7)(c)
(b)(6); (b)(7)(c)
[Redacted]

SOUTH CAROLINA

(b)(6); (b)(7)(c)
[Redacted]
Emergency Management Division
Pine Ridge Armory
2779 Fish Hatchery Road, West Columbia, SC 29172-2024
Fax: 803/737-8570
24-Hr: 803/737-8500

(b)(6); (b)(7)(c)
(b)(6); (b)(7)(c)
[Redacted]

SOUTH DAKOTA

Department of Public Safety
Office of Emergency Management
118 W. Capitol Avenue, Pierre, SD 57501
Ph: 605/773.32321
Fax: 605/773.3580
24-Hr: 605/773-3231

(b)(6); (b)(7)(c)
[Redacted]

TENNESSEE

Tennessee Emergency Management Agency
3041 Sidco Drive, Nashville, TN 37204-1502
Fax: 615/242-9635
24-Hr: 615/741-0001 & In-State: 800/262-3400,
Out-of-State: 800/258-3300

(b)(6); (b)(7)(c)
[Redacted]

September 25, 2009

FOR OFFICIAL USE ONLY

NCC SOP 303

(b)(6); (b)(7)(c)

TEXAS

Texas Department of Public Safety
Emergency Management Division
5805 North Lamar Blvd., Austin, Texas 78752-4422
Fax: 512/424-2444
24-Hr: 512/424-2208

(b)(6); (b)(7)(c)

UTAH

Department of Public Safety
Div. of Emergency Services and Homeland Security
State Office Building, Room 1110, Salt Lake City, UT 84114
Fax: 801/538-3770
24-Hr: 801/538-3400 or 1-800-SL-FAULT

(b)(6); (b)(7)(c)

VERMONT

Department of Public Safety
Emergency Management Division
103 S. Main Street, Waterbury, VT 05671-2101
Ph: 802/244-8721
Fax: 802/241-5556
24-Hr: 800/347-0488

(b)(6); (b)(7)(c)
(b)(6); (b)(7)(c)

VIRGINIA

(b)(6); (b)(7)(c)

Department of Emergency Management
10501 Trade Court Virginia, Richmond, VA 23236-3713
Fax: 804/897-6576
24-Hr: 804/674-2400 or 800/468-8892

(b)(6); (b)(7)(c)
(b)(6); (b)(7)(c)

WASHINGTON

Washington State Emergency Management
Building 20, Camp Murray
Tacoma, WA 98430
Ph: 800-562-6108
24-hr: 1-800-258-5990

(b)(6); (b)(7)(c)

September 25, 2009

FOR OFFICIAL USE ONLY

NCC SOP 303

(b)(6); (b)(7)(c)

WEST VIRGINIA

Division of Homeland Security and Emergency Management
Bldg. 1 Rm. EB-80, 1900 Kanawha Blvd. East, Charleston WV 25305
Ph: 304/558-5380
Fax: 304/558-4538
24-Hr: 800/342-3074

(b)(6); (b)(7)(c)

WISCONSIN

Wisconsin Emergency Management
2400 Wright Street, P.O. Box 7865, Madison, WI 53708
Ph: 608/242-3232
Fax: 608/242-3247
24-Hr: 800/943-0003 or 608/242-3232

(b)(6); (b)(7)(c)

WYOMING

Emergency Management Agency
Office of Homeland Security
624 E. Pershing, Cheyenne, WY 82001
Ph: 307/777-4663
Fax: 307/638-7670
24-Hr: 307/777-4321

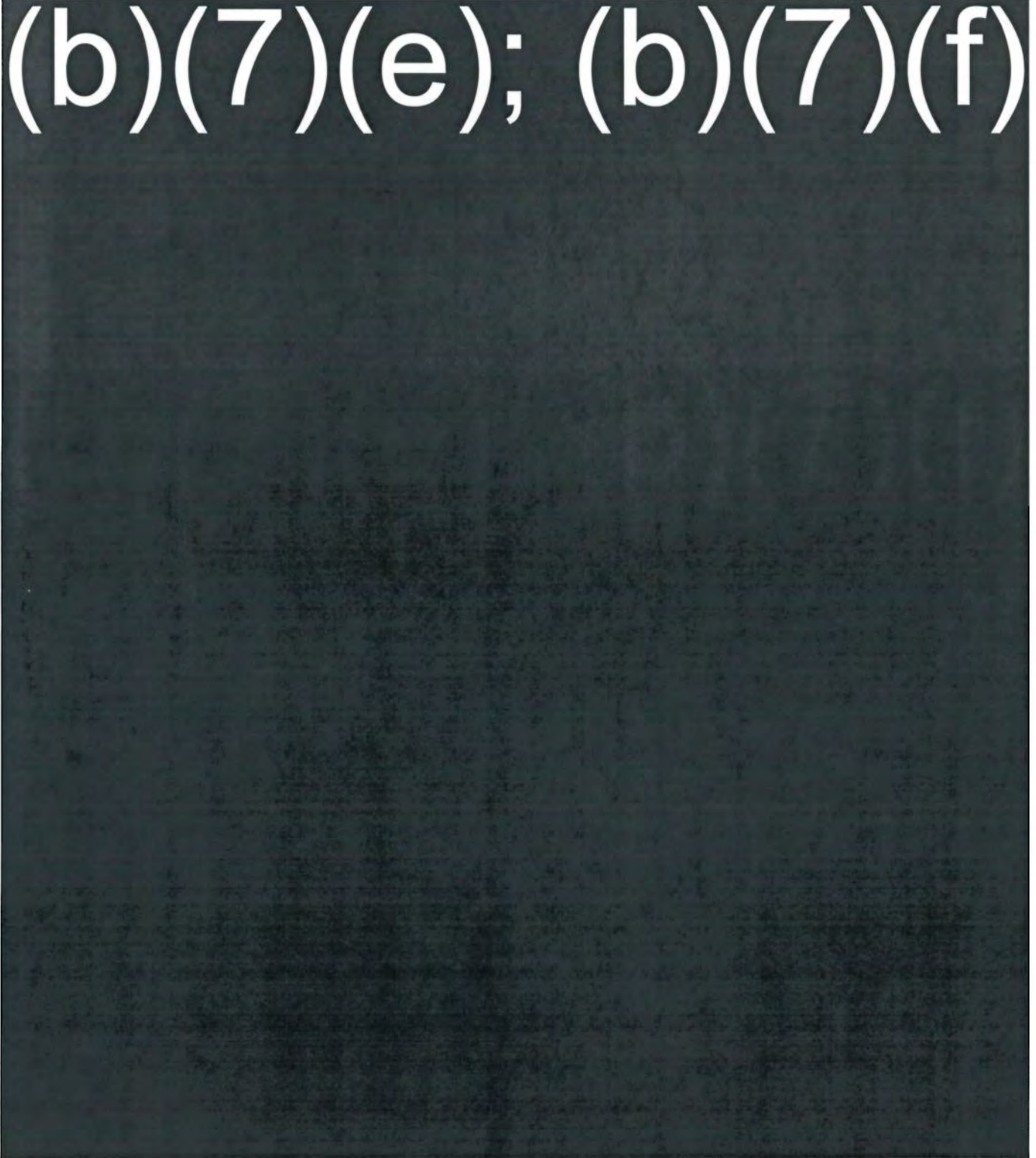
(b)(6); (b)(7)(c)

September 25, 2009

FOR OFFICIAL USE ONLY

NCC SOP 303

(b)(7)(e); (b)(7)(f)

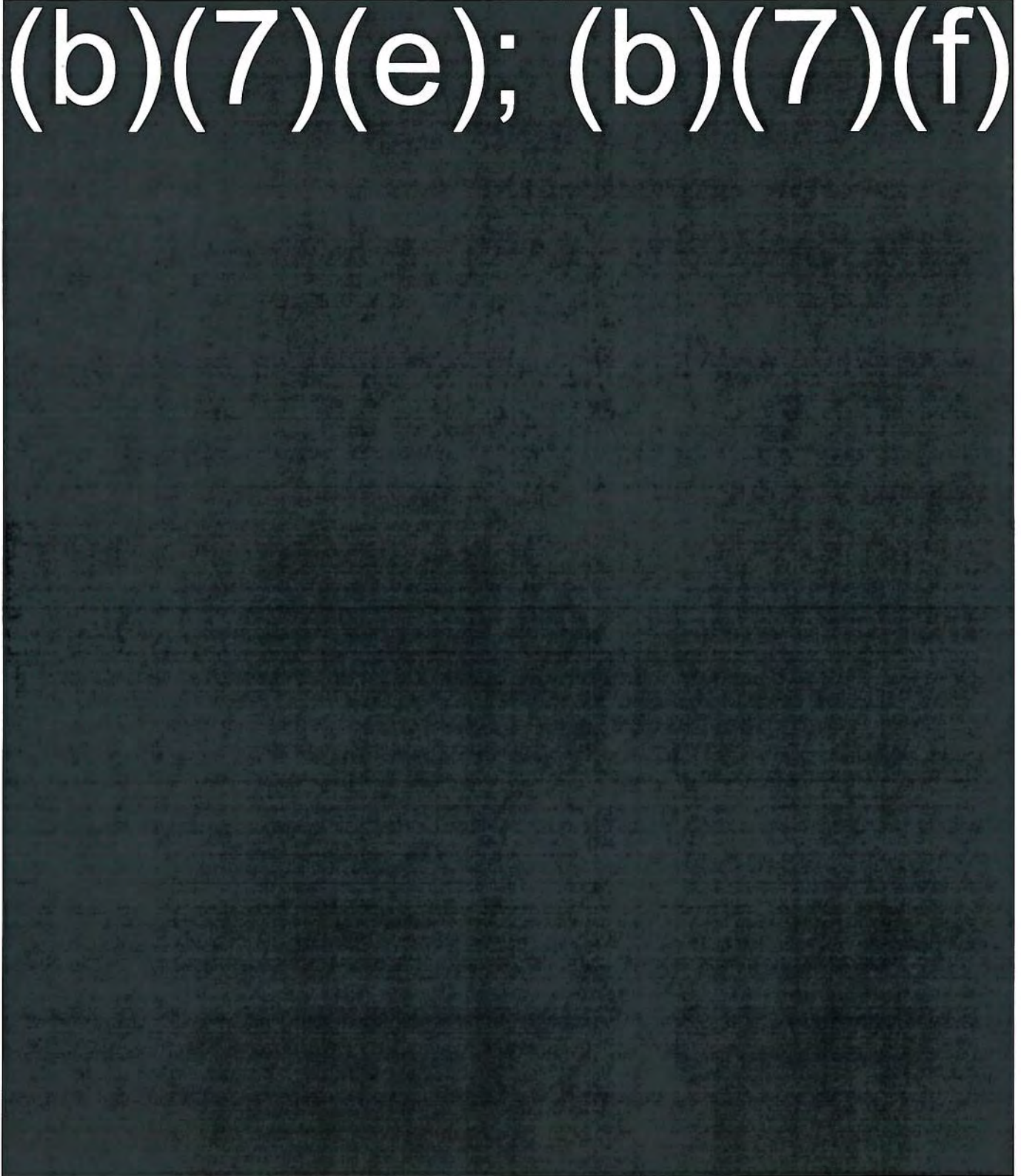


September 25, 2009

FOR OFFICIAL USE ONLY

NCC SOP 303

(b)(7)(e); (b)(7)(f)



Office of Primary Responsibility: NCC
Distribution: OMNCS, NCC, NOC, All POCs in Appendix A

Page 20 of 30

FOR OFFICIAL USE ONLY

September 25, 2009

FOR OFFICIAL USE ONLY

NCC SOP 303

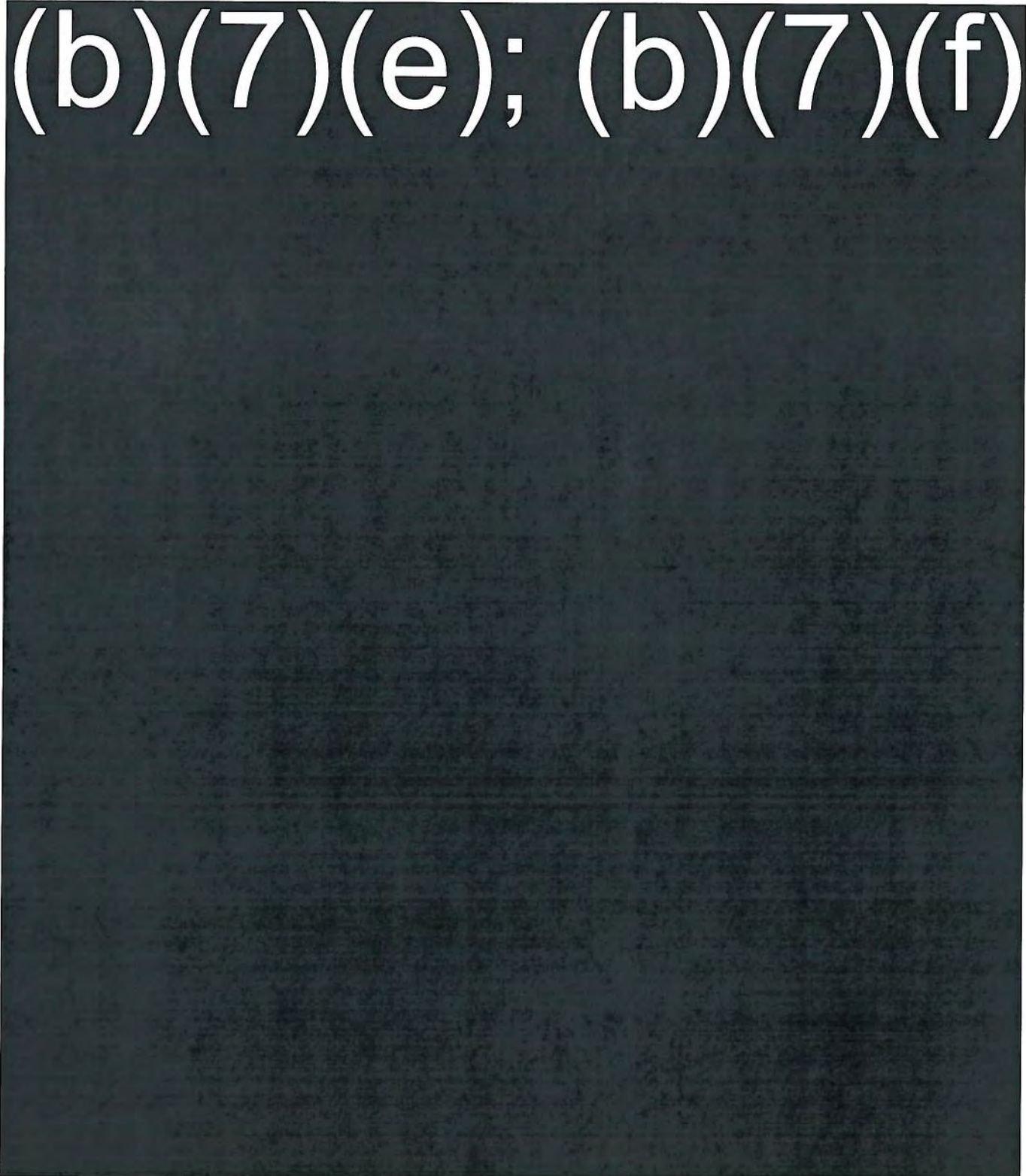
(b)(7)(e); (b)(7)(f)

September 25, 2009

FOR OFFICIAL USE ONLY

NCC SOP 303

(b)(7)(e); (b)(7)(f)

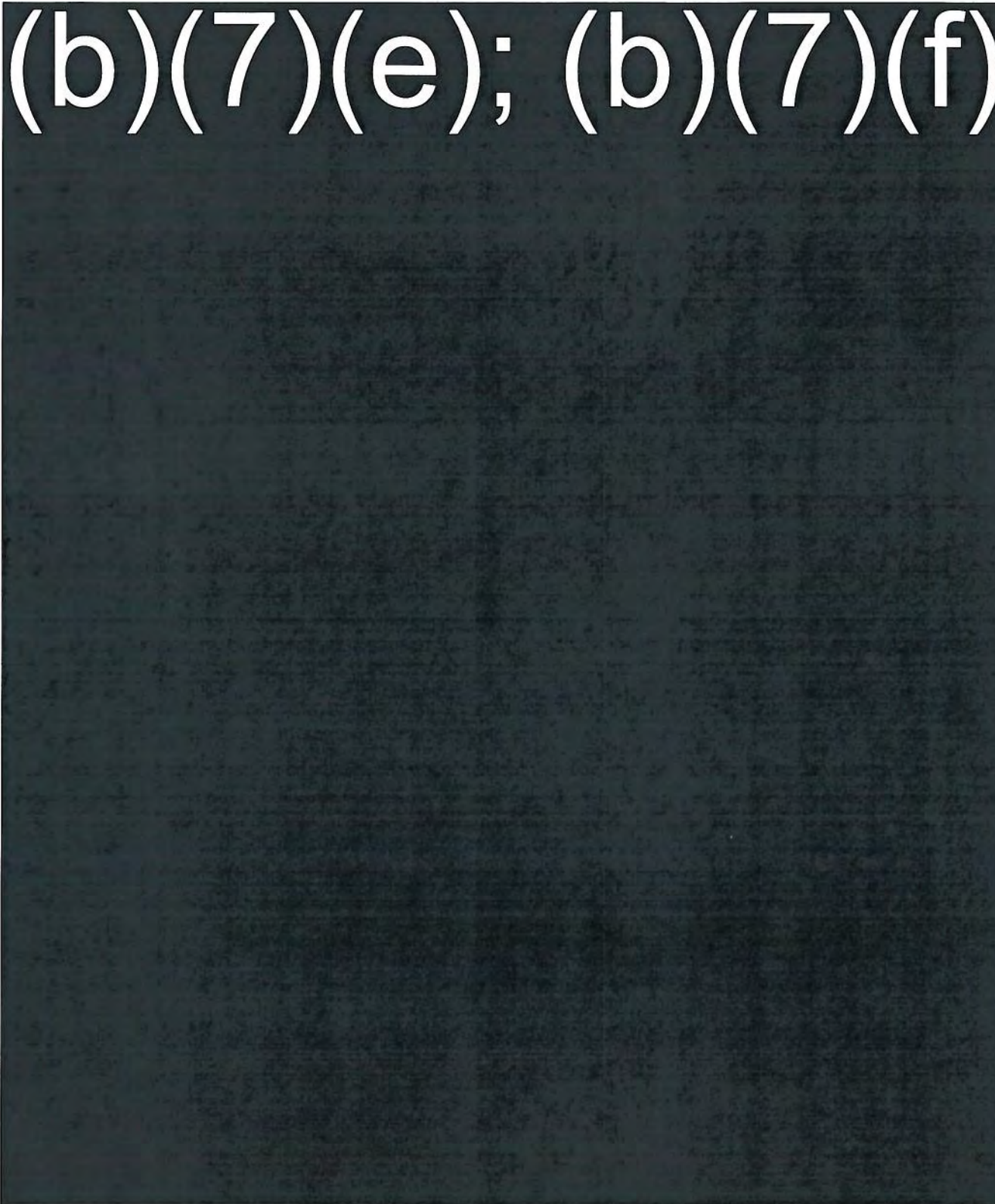


September 25, 2009

FOR OFFICIAL USE ONLY

NCC SOP 303

(b)(7)(e); (b)(7)(f)



Office of Primary Responsibility: NCC
Distribution: OMNCS, NCC, NOC, All POCs in Appendix A

Page 23 of 30

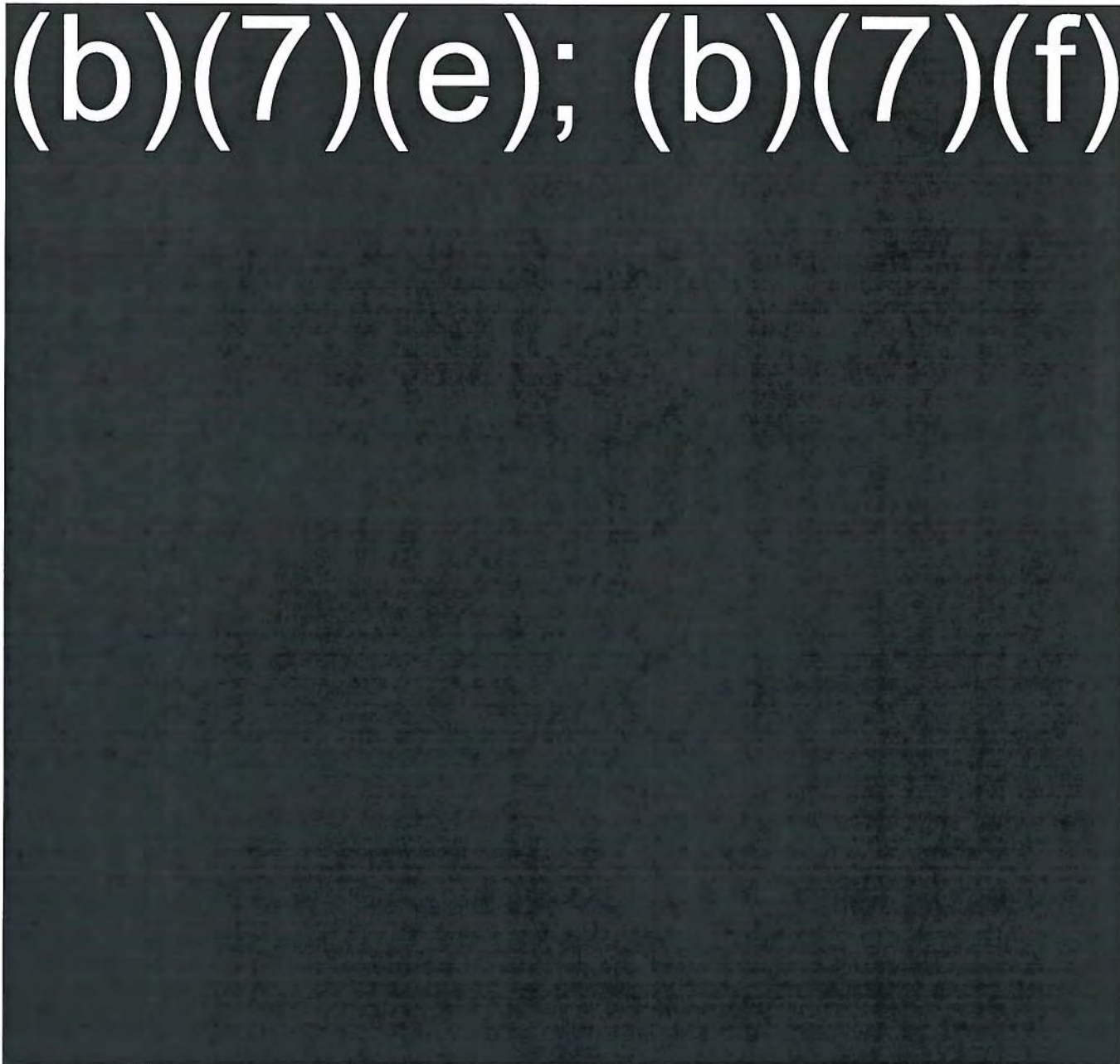
FOR OFFICIAL USE ONLY

September 25, 2009

FOR OFFICIAL USE ONLY

NCC SOP 303

(b)(7)(e); (b)(7)(f)

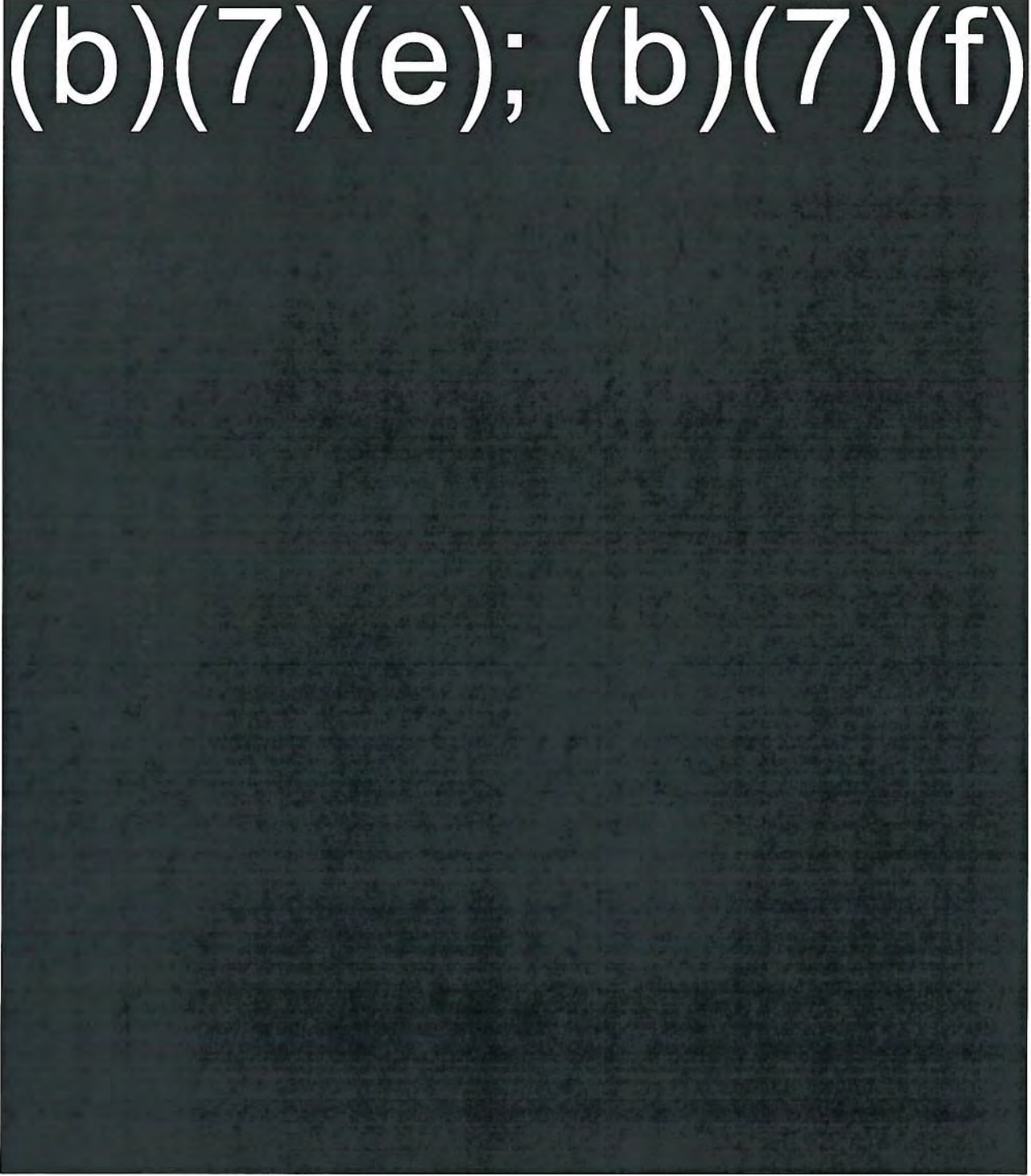


September 25, 2009

FOR OFFICIAL USE ONLY

NCC SOP 303

(b)(7)(e); (b)(7)(f)

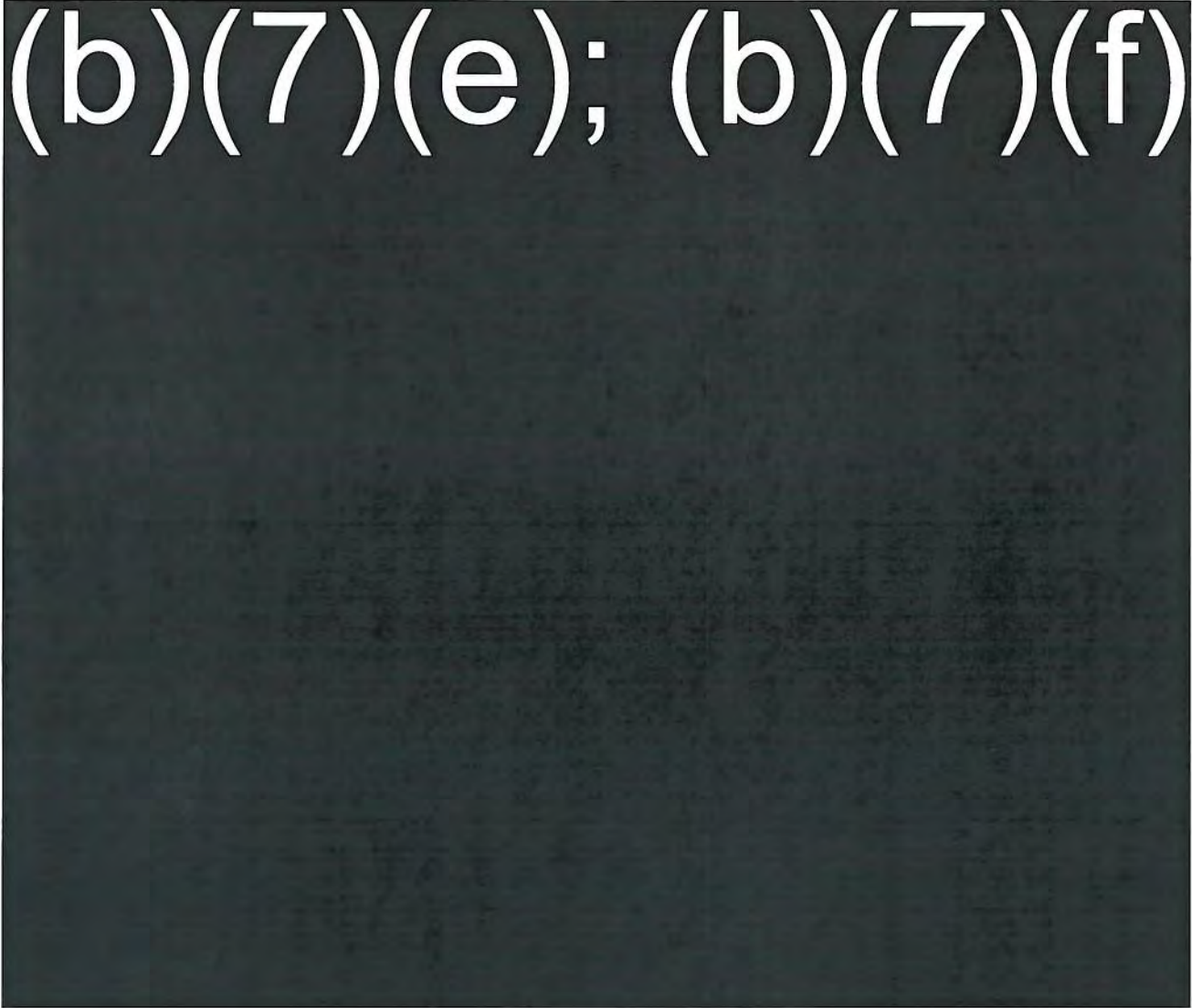


September 25, 2009

FOR OFFICIAL USE ONLY

NCC SOP 303

(b)(7)(e); (b)(7)(f)



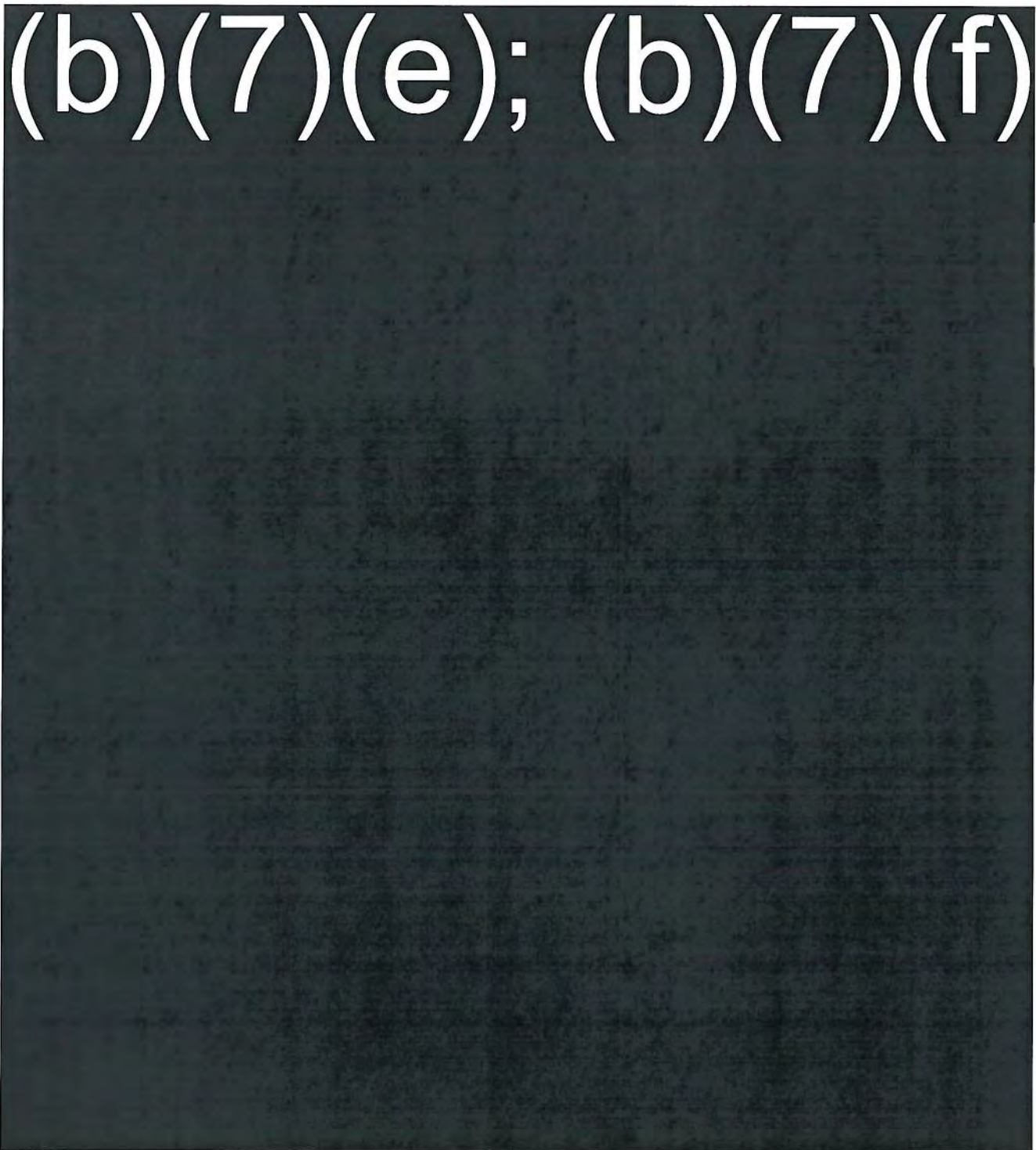
September 25, 2009

FOR OFFICIAL USE ONLY

NCC SOP 303

Appendix E: External Agency Cellular Service Disruption Implementation Instructions

(b)(7)(e); (b)(7)(f)

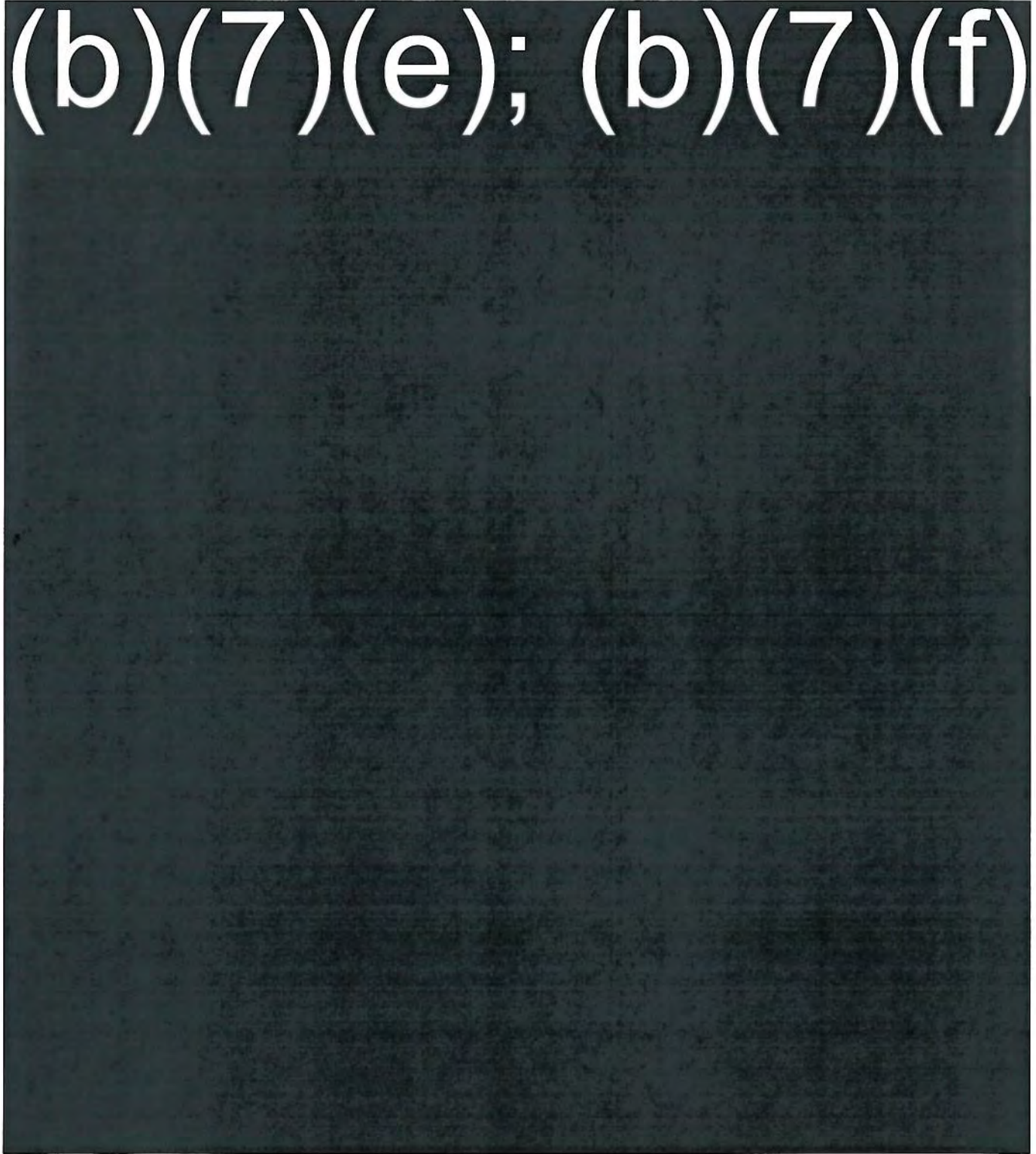


September 25, 2009

FOR OFFICIAL USE ONLY

NCC SOP 303

(b)(7)(e); (b)(7)(f)

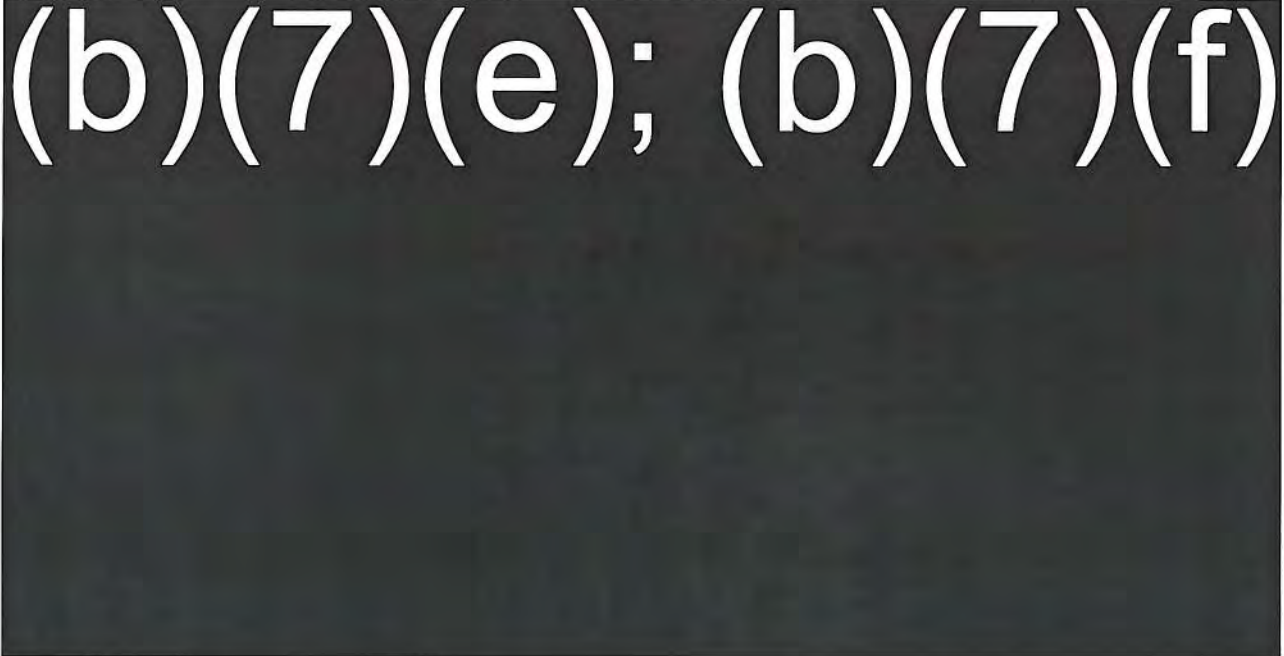


September 25, 2009

FOR OFFICIAL USE ONLY

NCC SOP 303

(b)(7)(e); (b)(7)(f)

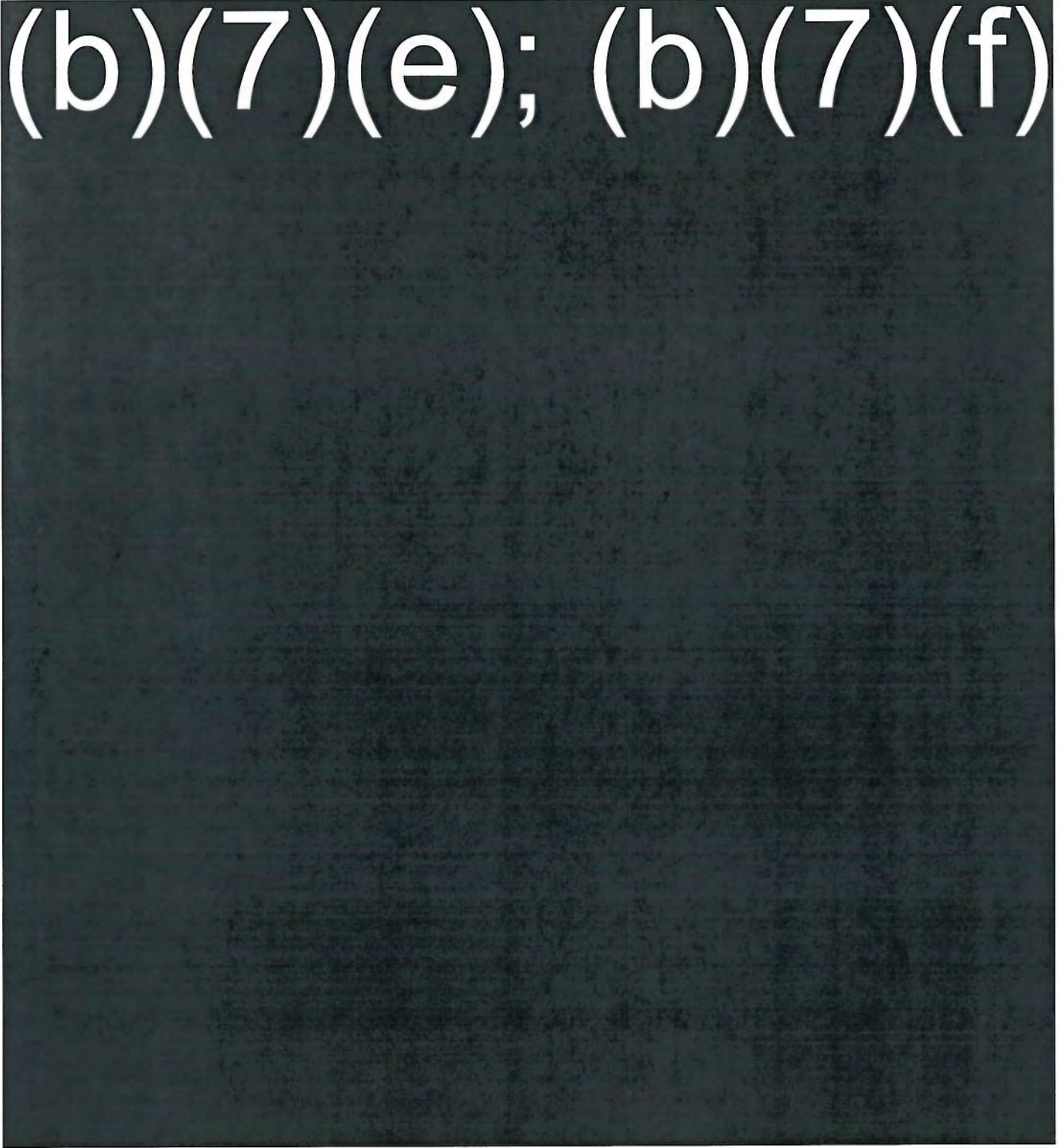


September 25, 2009

FOR OFFICIAL USE ONLY

NCC SOP 303

(b)(7)(e); (b)(7)(f)



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

)	
ELECTRONIC PRIVACY)	
INFORMATION CENTER,)	
)	
Plaintiff,)	
)	
v.)	
)	Case No. 1:13-CV-260 (JEB)
DEPARTMENT OF HOMELAND)	
SECURITY)	
)	
Defendant)	
)	

**PLAINTIFF’S STATEMENT OF DISPUTED MATERIAL FACTS AS TO
WHICH THERE IS A GENUINE ISSUE**

Pursuant to Local Civil Rule 7(h), Plaintiff Electronic Privacy Information Center (“EPIC”) submits the following statement of disputed and undisputed facts in opposition to Defendant Department of Homeland Security’s motion for summary judgment and in support of Plaintiff’s cross-motion for summary judgment. This statement identifies the portions of Defendant’s Statement of Material Facts Not In Dispute, Dkt. 10 at 19, as to which Plaintiff contends there exists a genuine issue.

1. Plaintiff agrees that there is no genuine issue as to the facts set forth in paragraphs 1, 3-20, 22, and 24 of Defendant’s Statement.
2. Plaintiff contends that there exist genuine issues of material fact as to the matters set forth in paragraphs 2, 21, 23, and 25 of Defendant’s Statement, as explained below.
3. Paragraph 2 of Defendant’s Statement asserts that “Standard Operating Procedure (SOP) 303 is a document that details a process for the ‘deactivation of wireless networks’ primarily to ‘deter the triggering of radio-activated improvised explosive devices.’” Defs.’ Statement ¶ 3. Plaintiff does not dispute that SOP 303 *includes* details of a process to “deactivate wireless networks,” but Plaintiff asserts that there is a genuine issue as to whether details of the deactivation process are *all* that is included in SOP 303.

4. In support of this assertion, Plaintiff has attached pages from the President's National Security Telecommunications Advisory Committee's 2006-2007 Report on "Termination of Cellular Networks During Emergency Situations." Exhibit 1. This report indicates [thing].
5. Paragraph 21 of Defendant's Statement asserts that DHS determined that "SOP 303 is a record compiled for law enforcement purposes and the release of portions of SOP 303 would disclose the techniques and procedures for law enforcement investigations," and that DHS invokes Exemption 7(E) to justify this withholding. Defs.' Statement at ¶ 21. Plaintiff disputes the adequacy of the explanation for these conclusions.
6. Paragraph 23 of Defendant's Statement asserts that DHS determined that "SOP 303 is a record compiled for law enforcement purposes and the release of portions of SOP 303 could reasonably be expected to endanger the life or safety of an individual," and that DHS invokes Exemption 7(F) to justify this withholding. Defs.' Statement at ¶ 23-4. Plaintiff disputes these conclusions because the agency has failed to identify an identifiable individual or individuals whose safety would be threatened by disclosure, and because the threat invoked by DHS is hypothetical and only tangentially related to the safety of the unidentified individuals.
7. Paragraph 25 of Defendant's Statement asserts, "The agency determined that portions of SOP 303 are non-exempt, and it is releasing those portions to EPIC." Defs.' Statement at ¶ 23. Plaintiff does not dispute that those portions of SOP 303 are non-exempt, but Plaintiff asserts that there is a genuine issue as to whether Defendant has conducted a sufficient segregability analysis to identify *all* non-exempt portions of SOP 303.

Termination of Cellular Networks During Emergency Situations

Investigation Group / Period of Activity

Cellular Service Shutdown Ad Hoc Working Group

August 2005 – January 2006

Issue Background

As a direct result of the bombings that took place in the London transportation system in July 2005, U.S. authorities initiated the shut down of cellular network services in the Lincoln, Holland, Queens, and Brooklyn Battery Tunnels. The Federal Government based this precautionary measure on the suspicion that similar attacks might also be perpetrated in the tunnels leading to and from New York City. Though the decision was rooted in vital security concerns, the resulting situation, undertaken without prior notice to wireless carriers or the public, created disorder for both Government and the private sector at a time when use of the communications infrastructure was most needed. Shortly following these activities, the National Coordinating Center (NCC) hosted a teleconference to discuss the need to develop a process for determining if and when cellular shutdown activities should be undertaken in the future in light of the serious impact these efforts could have had, not only on access by the public to emergency communications services during these situations, but also on public trust in the communications infrastructure in general.

History of NSTAC Actions and Recommendations

These actions highlighted, within the President's National Security Telecommunications Advisory Committee (NSTAC) community, the need for a process to ensure that future similar decisions meet the Nation's security goals and ensure the protection of critical infrastructures. Consequently, on August 18, 2005, the NSTAC established a Principal level task force to formulate, on an expedited basis, recommendations to effect efficient coordinated action between industry and Government in times of national emergency.

To facilitate more coordinated action, the NSTAC recommended that the President direct his departments and agencies to:

- Work to implement a simple process, building upon existing processes, with the Department of Homeland Security (DHS) and National Communications System (NCS) coordination enabling the Government to speak with one voice, provide decision makers with relevant information, and provide wireless carriers with Government-authenticated decisions for implementation; and
- Achieve rapid implementation through the Homeland Security Advisor of each State, in conjunction with the NCS and the Office of State and Local Government Coordination, DHS.

The group concluded its activities upon NSTAC approval of the Letter and recommendations in January 2006.

Actions Resulting from NSTAC Recommendations

In support of the recommendations, the NCS approved Standard Operating Procedure (SOP) 303, "Emergency Wireless Protocols," on March 9, 2006, codifying a shutdown and restoration process for use by commercial and private wireless networks during national crises. Under the process, the NCC will function as the focal point for coordinating any actions leading up to and following the termination of private wireless network connections, both within a localized area, such as a tunnel or bridge, and within an entire metropolitan area. The decision to shutdown service will be made by State Homeland Security Advisors, their designees, or representatives of the DHS Homeland Security Operations Center. Once the request has been made by these entities, the NCC will operate as an authenticating body, notifying the carriers in the affected area of the decision. The NCC will also ask the requestor a series of questions to determine if the shutdown is a necessary action. After making the determination that the shutdown is no longer required, the NCC will initiate a similar process to reestablish service. The NCS continues to work with the Office of State and

Local Government Coordination at DHS, and the Homeland Security Advisor for each State to initiate the rapid implementation of these procedures.

Reports Issued

NSTAC Cellular Shutdown Letter to the President, January 2006

**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/>)	

[PROPOSED] ORDER

Upon consideration of Defendant’s Motion for Summary Judgment, Plaintiffs’ Cross-Motion for Summary Judgment, and related filings, it is hereby:

ORDERED that Defendants’ Motion for Summary Judgment is DENIED;

ORDERED that Plaintiffs’ Cross-Motion for Summary Judgment is GRANTED;

ORDERED that Defendant shall produce all records responsive to Plaintiff’s Freedom of Information Act request

Dated: _____.

JAMES E. BOASBERG
United States District Judge