

[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

JOINT APPENDIX

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*

TABLE OF CONTENTS

	Page
Complaint (Dkt. No. 1)	JA 1
Declaration of James V.M.L. Holzer, I, In Support of Defendant's Motion for Summary Judgment (Dkt. No. 10-2).....	JA 10
FOIA Administrative Appeal and Exhibits (Dkt. No. 10-4)	JA 20
Appendix 1, EPIC's July 10, 2012 FOIA Request to DHS.....	JA 24
Appendix 2, DHS's July 24, 2012 Acknowledgement of EPIC's FOIA Request.....	JA 30
Appendix 3, DHS's August 21, 2012 Final Determination on EPIC's FOIA Request.....	JA 33
Administrative Decision Remanding FOIA Request (Dkt. No. 10-5)	JA 36
<i>Vaughn</i> Index (Dkt. No. 10-6)	JA 38
President's Nat'l Sec. Advisory Comm., <i>Termination of Cellular Networks During Emergency Situations</i> (Dkt. No. 11-4)	JA 39
Order (Dkt. No. 18)	JA 41
Memorandum Opinion (Dkt. No. 19)	JA 42
Notice of Appeal (Dkt. No. 21).....	JA 58

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

<hr/>)
ELECTRONIC PRIVACY INFORMATION CENTER)
1718 Connecticut Ave., NW)
Suite 200)
Washington, DC 20009)
)
Plaintiff,)
)
v.)
	Civil Action No. _____)
DEPARTMENT OF HOMELAND SECURITY)
Washington, DC 20528)
)
Defendant)
<hr/>)

COMPLAINT FOR INJUNCTIVE RELIEF

1. This is an action under the Freedom of Information Act (“FOIA”), 5 U.S.C. § 552 (2012), for injunctive and other appropriate relief, seeking the release of agency records requested by the Electronic Privacy Information Center (“EPIC”) from the Department of Homeland Security (“DHS”).

2. This lawsuit challenges the failure of DHS to disclose documents in response to EPIC's July 10, 2012, Freedom of Information Act request. EPIC's FOIA Request sought agency records related to specific communications shutdown procedures (“Standard Operating Procedure 303” or “SOP 303”) approved by the National Communications System. Defendant has failed to comply with its statutory deadline and has failed to disclose a single record. EPIC asks the Court to order immediate disclosure of all responsive records.

Jurisdiction and Venue

3. This Court has subject matter jurisdiction over this action and personal jurisdiction over the parties pursuant to 5 U.S.C. § 552(a)(4)(A)(vii), 5 U.S.C. § 552(a)(4)(B), and 5 U.S.C. § 552(a)(6)(C)(i) (2012). This Court also has jurisdiction over this action pursuant to 28 U.S.C. § 1331 (2012). Venue is proper in this district under 5 U.S.C. § 552(a)(4)(B) (2012).

Parties

4. Plaintiff EPIC is a public interest research organization incorporated as a not-for-profit corporation in Washington, D.C. EPIC conducts oversight of government activities and policies and analyzes their impact on civil liberties and privacy interests. Among its other activities, EPIC publishes books, reports, and a bi-weekly electronic newsletter. EPIC also maintains a popular Internet site, <http://www.epic.org>, which contains extensive information on current privacy issues, including documents obtained from federal agencies under the FOIA. EPIC routinely and systematically disseminates information to the public through its website and other media outlets. This Court recognized EPIC's role as a representative of the news media in *EPIC v. Dep't of Defense*, 241 F. Supp. 2d. 5 (D.D.C. 2003).

5. Defendant DHS is a Department of the Executive Branch of the U.S. government and an agency within the meaning of 5 U.S.C. § 552(f)(1). Until President Obama dissolved the NCS through Executive Order 13618 on July 6, 2012, DHS included a component called the National Communications System ("NCS"). In turn, the NCS oversaw the work of two sub-components: the President's National Security Telecommunications Advisory Committee ("NSTAC") and the National Coordinating Center ("NCC").

FACTS

NCS Approved Standard Operating Procedure 303

6. In its 2006-2007 Issue Review, the NSTAC revealed that it had approved SOP 303, although the details of SOP 303 were not released to the public.
7. The Issue Review explained that SOP 303 codifies “a shutdown and restoration process for use by commercial and private wireless networks during national crises.”
8. The Issue Review further explained that SOP 303 would be implemented under the coordination of the NCC
9. The decision to shut down service would be made by State Homeland Security Advisors or “representatives of the DHS Homeland Security Operations Center,” but would require the permission of the NCC. The Review states, “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.”
10. The Issue Review indicates that NCC will determine whether a shutdown is necessary by asking the requestor “a series of questions.” The NCC will follow the same procedure in order to reestablish service “[a]fter making the determination that the shutdown is no longer required.
11. On July 3, 2011, a Bay Area Rapid Transit (“BART”) officer in San Francisco, CA, shot and killed a homeless man, Charles Hill. The officer alleged later that Hill had attacked him with a knife and that he had acted in self-defense.
12. The death sparked a major protest against BART on July 11, 2011. Though the protests interrupted BART service at several transit stations, no one was injured.
13. A second protest was planned one month later, on August 12, 2011. However, this protest was cut short after BART officials cut off all cellular service inside four transit

stations for a period of three hours. This act prevented any individual on the station platform from sending or receiving phone calls, messages, or other data.

14. A 2011 Report from the White House asserted that the National Security Council and the Office of Science and Technology Policy have the legal authority to control private communications systems in the United States during times of war or other national emergencies.

15. On April 30, 2012, the Federal Communications Commission requested public comment on proposed procedures to guide “intentional interruption of wireless service by government actors for the purpose of ensuring public safety.”

16. On July 6, 2012, the White House approved an Executive Order seeking to ensure the continuity of Government communications during a national crisis. As part of the Executive Order, DHS was granted the authority to seize private facilities, when necessary, effectively shutting down or limiting civilian communications.

EPIC’s FOIA Request

17. Paragraphs 1-16 above are hereby incorporated by reference as if set forth fully herein.

18. On July 10, 2012, EPIC transmitted, via certified mail, a FOIA request to the Chief Privacy Officer/Chief FOIA Officer in the Privacy Office at DHS, seeking records (“EPIC’s FOIA Request”).

19. EPIC’s FOIA Request asked for the following agency records:

- a) The full text of Standard Operating Procedure 303;
- b) The full text of the pre-determined “series of questions” that determines if a shutdown is necessary;

- c) 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.

20. In the Request, EPIC asked the DHS to expedite its response to the Request because EPIC is primarily engaged in disseminating information and the request pertained to a matter about which there was an urgency to inform the public about an actual or alleged government activity. EPIC made this request pursuant to 5 U.S.C. § 552(a)(6)(E)(v)(II). EPIC based such a request on the urgency for the public to obtain information about DHS' authority to approve the shutdown of wireless networks in the United States. To illustrate this public interest need, EPIC cited extensive news coverage of the July 6, 2012 Executive Order that granted DHS expanded authority to seize control of private communications facilities during times of national crisis, as well as coverage of numerous cybersecurity bills under consideration that would extend DHS' cyber authority.

21. In the Request, EPIC also requested "News Media" fee status under the FOIA based on its status as a "representative of the news media." EPIC further requested waiver of all duplication fees because disclosure of the records requested will contribute significantly to public understanding of the operations or activities of the government.

22. On July 24, 2012, DHS acknowledged receipt of EPIC's FOIA Request.

23. In its acknowledgment, DHS responded that it would conditionally grant a fee waiver, based on a "sampling of the responsive documents received from the various DHS program offices as a result of the searches conducted in response" to EPIC's Request.

24. In its acknowledgment, DHS did not make a determination as to EPIC's request for expedited processing, but invoked a 10-day extension due to the "unusual circumstance" that EPIC's FOIA Request is "of substantial interest" to two or more components of DHS or another agency.

25. DHS also indicated that the appropriate components had been queried.

26. DHS assigned EPIC's FOIA Request reference number DHS/OS/PRIV 12-0598.

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

28. On September 13, 2012, EPIC transmitted, via certified mail, an administrative appeal to DHS ("EPIC's Administrative Appeal"), appealing the sufficiency of the DHS' search regarding EPIC's FOIA Request.

29. EPIC's Administrative Appeal also challenged DHS's practice of politically vetting FOIA requests and requested that DHS explain why the Request was "of substantial interest," what "substantial interest" indicated in this context, and which entities were consulted prior to the issuance of a final determination on the substance of EPIC's FOIA Request.

30. EPIC's Administrative Appeal noted the reference number assigned to EPIC's FOIA Request by DHS.

31. EPIC's Administrative Appeal renewed EPIC's request for "News Media" fee status and a waiver of all duplication fees.

32. EPIC's Administrative Appeal also renewed EPIC's request for expedited treatment, and requested expedited treatment of the Appeal.

33. In a letter dated October 25, 2012, DHS acknowledged EPIC's Administrative Appeal.

34. DHS assigned the Administrative Appeal reference number 2013-HQAP-00004.

35. In its October 25 letter, DHS further stated that there would be delay in resolving EPIC's Administrative Appeal, since DHS had received "a high number of FOIA requests" and was experiencing a "backlog."

36. As of November 23, 2012, DHS has failed to make a determination with respect to EPIC's Appeal within twenty days after receipt of the appeal, as prescribed by 5 U.S.C. § 552(a)(6)(A)(ii) (2012).

37. Through the date of this pleading, DHS has failed to produce any documents in response to EPIC's FOIA Request.

38. DHS's failure to respond within the twenty-day statutory limit constitutes a constructive denial of EPIC's Appeal.

Count I

Violation of FOIA: Failure to Comply With Statutory Deadlines

39. Paragraphs 1-38 above are hereby incorporated by reference as if set forth fully herein.

40. As described above, Defendant DHS' failure to respond to EPIC's Administrative Appeal violated the statutory deadline imposed by the FOIA set forth in 5 U.S.C. § 552 (a)(6)(A)(ii).

41. EPIC has exhausted the applicable administrative remedies with respect to EPIC's FOIA Request. 5 U.S.C. § 552(a)(4)(B).

42. EPIC is entitled to injunctive relief compelling the release and disclosure of the requested agency records.

Count II

Violation of FOIA: Failure to Make Reasonable Efforts to Search for Responsive Records

43. Paragraphs 1-42 above are hereby incorporated by reference as if set forth fully herein.

44. As described above, DHS's failure to make reasonable efforts to search for responsive documents violates FOIA, 5 U.S.C. § 552(a)(3)(C).

45. EPIC has exhausted the applicable administrative remedies with respect to EPIC's FOIA Request. 5 U.S.C. § 552(a)(4)(B).

46. EPIC is entitled to injunctive relief compelling the release and disclosure of the requested agency records.

Count III

Violation of FOIA: Unlawful Withholding of Agency Records

47. Paragraphs 1-46 above are hereby incorporated by reference as if set forth fully herein.

48. As described above, DHS has failed to comply with statutory deadlines and failed to make responsive records available to EPIC.

49. As a result of DHS' unlawful delay and failure to conduct a reasonable search, the agency has withheld responsive agency records from EPIC in violation of FOIA, 5 U.S.C. § 552(a)(3)(A).

50. EPIC has exhausted the applicable administrative remedies with respect to EPIC's FOIA Request. 5 U.S.C. § 552(a)(4)(B).

51. EPIC is entitled to injunctive relief compelling the release and disclosure of the requested agency records.

Requested Relief

WHEREFORE, Plaintiff prays that this Court:

- A. order Defendant to conduct a reasonable search for all responsive records;
- B. order Defendant to promptly disclose to Plaintiff responsive agency records;
- C. award Plaintiff its costs and reasonable attorneys' fees incurred in this action pursuant to 5 U.S.C. § 552(a)(4)(E) (2010); and
- E. grant such other relief as the Court may deem just and proper.

Respectfully submitted,

By: 

Ginger McCall, Esquire (DC Bar #1001104)

David Jacobs, Esquire*

Julia Horwitz, Esquire**

ELECTRONIC PRIVACY INFORMATION
CENTER

1718 Connecticut Avenue, N.W.

Suite 200

Washington, D.C. 20009

(202) 483-1140 (telephone)

(202) 483-1248 (facsimile)

Dated: February 27, 2013

* David Jacobs is barred in New York State.

** Julia Horwitz is barred in Maryland.

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

ELECTRONIC PRIVACY INFORMATION)
CENTER,)
) Civil Action No. 13-260 (GK)
Plaintiff,)
)
v.)
)
U.S. DEPARTMENT OF HOMELAND)
SECURITY)
)
Defendant.)
_____)

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

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

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

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

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

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

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

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

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

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

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

EPIC'S JULY 10, 2012 FOIA REQUEST

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

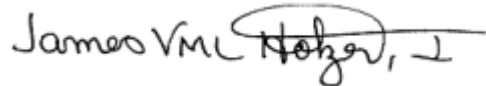
25. FOIA Exemption b(7)(e) permits the withholding of law enforcement information that "would disclose techniques and procedures for law enforcement investigations." The b(7)(e) exemption applies because the requested document contains a homeland security procedure primarily intended to efficiently and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

executed.

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

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

Executed this 28th day of June, 2013.



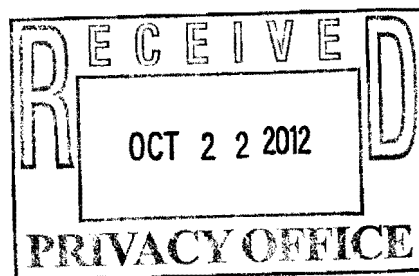
James V.M.L. Holzer

epic.org

September 13, 2012

VIA CERTIFIED MAIL

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



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

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

To Whom it May Concern:

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

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

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

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

DHS acknowledged EPIC's FOIA Request by letter dated July 24, 2012.² DHS did not make a determination as to EPIC's request for expedited processing, but invoked a 10-day extension due to the "unusual circumstance" that EPIC's FOIA Request is "of substantial interest" to two or more components of DHS or another agency. DHS conditionally granted EPIC's fee waiver request, indicated that the appropriate

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

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

component had been queried, and assigned EPIC's FOIA Request reference number DHS/OS/PRIV 12-0598.³

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

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

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

EPIC's FOIA Request firmly established the identity and existence of SOP 303.⁸ A publicly available document explains that SOP 303 was approved by the National Communications System ("NCS"), in 2006.⁹ NCS was first formed in 1962, but was transferred to DHS in 2003 and became part of DHS' "Directorate for Preparedness" under the Information Analysis and Infrastructure Sharing and Analysis Center in 2005.¹⁰ Many of the NCS programs are now led by the DHS Office of Cybersecurity and Communications within the National Protection and Programs Directorate.¹¹

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

³ *Id.*

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

⁵ *Id.*

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

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

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

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

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

¹¹ *Id.*

¹² See Letter from Mia Day, *supra* note 4 at 1.

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

EPIC Appeals DHS’ Treatment of EPIC’s FOIA Request

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

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

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

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

¹³ Letter from Marc Rotenber, Executive Director, EPIC, et al, to the Honorable Darrell E. Issa, Chairman, House Committee on Oversight and Government Reform and the Honorable Elijah Cummings, Ranking Member, House Committee on Oversight and Government Reform (Feb. 15, 2011), *available at* http://epic.org/open_gov/foia/Issa_FOIA_Oversight_Ltr_02_15_11.pdf.

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

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

EPIC Renews Its Request for “News Media” Fee Status

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

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

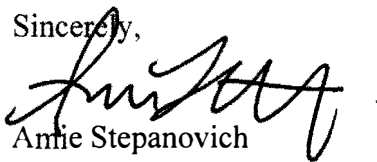
EPIC Renews Its Request for Expedited Treatment and Requests Expedited Treatment of this Appeal

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

Conclusion

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

Sincerely,



Annie Stepanovich
Associate Litigation Counsel
Electronic Privacy Information Center

/enclosures

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

Appendix 1

EPIC's July 10, 2012 FOIA Request to DHS

epic.org

July 10, 2012

VIA CERTIFIED MAIL

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

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

Re: Freedom of Information Act Request

To Whom it May Concern:

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

Background

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

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

¹ 5 U.S.C. § 552 (2011).

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

³ *Id.* at 139.

⁴ *Id.* at 139-40.

⁵ *Id.* at 139.

⁶ *BART Protests: San Francisco Transit Cuts Cellphones to Thwart Demonstrators; First Amendment Debate*, Ned Potter, ABC News, Aug. 16, 2011 <http://abcnews.go.com/Technology/bart-protest-san-francisco-transit-cut-cellphones-prevent/story?id=14311444#.T9jZ1vF2m5Y>.

attacked him with a knife and that he had acted in self-defense.⁷ The death sparked a major protest against BART on July 11, 2011.⁸ Though the protests disrupted service at several transit stations, no one was injured.⁹ A second protest was planned one month later, but was cut short after BART officials cut off all cellular service inside four transit stations for a period of three hours.¹⁰ This act prevented any individual on the station platform from sending or receiving phone calls, messages, or other data.¹¹

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

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

⁷ *Id.*

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

⁹ *Id.*

¹⁰ Potter, *supra* note 6.

¹¹ *Id.*

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

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

¹⁴ *Id.* at Sec. 5.2(e).

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

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

Documents Requested

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

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

Request for Expedited Processing

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

EPIC is “primarily engaged in disseminating information.”¹⁹

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

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

¹⁷ *Id.*

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

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

²⁰ White House, *supra* note 13.

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

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

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

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

Request for "News Media" Fee Status and Fee Waiver

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

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

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

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

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

²⁴ 6 C.F.R. § 5.11(c)(1)(i) (2011).

²⁵ *Id.* at (k)(1).

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

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

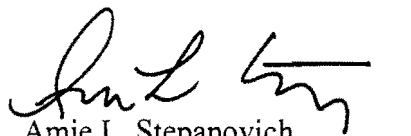
²⁸ See EPIC: EPIC v. Department of Homeland Security: Media Monitoring, <http://epic.org/foia/epic-v-dhs-media-monitoring/> (last visited July 9, 2012).

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

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

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

Respectfully Submitted,



Amie L. Stepanovich
Associate Litigation Counsel
Electronic Privacy Information Center

John J. Sadlik
IPIOP Clerk
Electronic Privacy Information Center

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

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

Appendix 2

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



Homeland Security

Privacy Office, Mail Stop 0655

July 24, 2012

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

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

Dear Ms. Stepanovich:

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

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

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

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

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

JA 31

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

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

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

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

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

Sincerely,



Mia Day
FOIA Program Specialist

3

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

JA 33



Homeland Security

Privacy Office, Mail Stop 0655

August 21, 2012

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

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

Dear Ms. Stepanovich:

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

You are seeking the following records:

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

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

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

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

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

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

Sincerely,

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

Mia Day
FOIA Program Specialist

U.S. Department of
Homeland Security

United States
Coast Guard



Office of the Administrative Law Judge
United States Coast Guard

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

5720
March 25, 2013

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

RE: DHS FOIA APPEAL 2013-HQAP-00004

Dear Ms. Stepanovich:

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

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

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

Sincerely,

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

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

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

JA 36

U.S. Department of
Homeland Security

United States
Coast Guard



Office of the Administrative Law Judge
United States Coast Guard

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

5720
March 25, 2013

MEMORANDUM

From: Joanna M. Sherry *JA*
Attorney Advisor

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

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

Subj: DHS FOIA APPEAL 2013-HQAP-00004

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

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

Enclosure: Remand Letter

JA 37

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

Vaughn Index

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

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

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

**ELECTRONIC PRIVACY
INFORMATION CENTER,**

Plaintiff,

v.

**DEPARTMENT OF HOMELAND
SECURITY,**

Defendant.

Civil Action No. 13-260 (JEB)

ORDER

As set forth in the accompanying Memorandum Opinion, the Court ORDERS that:

1. Defendant's Motion for Summary Judgment is DENIED;
2. Plaintiff's Motion for Summary Judgment is GRANTED;
3. This Judgment is STAYED for 30 days; and
4. Should DHS notice an appeal by December 12, 2013, the stay shall remain in effect until the Court of Appeals rules on such appeal.

IT IS SO ORDERED.

/s/ James E. Boasberg
JAMES E. BOASBERG
United States District Judge

Date: November 12, 2013

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

**ELECTRONIC PRIVACY
INFORMATION CENTER,**

Plaintiff,

v.

**DEPARTMENT OF HOMELAND
SECURITY,**

Defendant.

Civil Action No. 13-260 (JEB)

MEMORANDUM OPINION

This case concerns efforts of the Electronic Privacy Information Center under the Freedom of Information Act to obtain documents related to the Department of Homeland Security's Standard Operating Procedure 303. This protocol governs the shutdown of wireless networks in emergencies to, *inter alia*, prevent the remote detonation of explosive devices. After DHS withheld the lion's share of the one responsive document it found, EPIC brought this action. DHS now moves for summary judgment, arguing that its search for documents was adequate, that it properly withheld the bulk of SOP 303 under applicable FOIA exemptions, and that no other non-exempt parts of the document could be released. EPIC cross-moves for summary judgment, contending that the two exemptions DHS relied on to withhold most of the document, 7(E) and 7(F), do not apply here. As the Court believes EPIC has the better of this argument, it will dispose of the Motions accordingly.

I. Background

Standard Operating Procedure 303 is an "Emergency Wireless Protocol[] . . . codifying a shutdown and restoration process for use by commercial and private wireless networks during

national crises.” National Security Telecommunications Advisory Committee, NSTAC Issue Review 2006-07 at 139 (2007), http://www.dhs.gov/sites/default/files/publications/2006-2007%20NSTAC%20Issue%20Review_0.pdf. The wireless networks could be shut down in certain emergency situations to, *inter alia*, “deter the triggering of radio-activated improvised explosive devices.” See Def. Mot., Exh. 2 (Declaration of James V.M.L. Holzer), ¶ 25.

On July 10, 2012, EPIC submitted a FOIA request to DHS seeking: “(1) the full text of Standard Operating Procedure 303 (SOP 303), which describes a shutdown and restoration process for use by ‘commercial and private wireless networks’ in the event of a crisis; (2) the full text of the pre-determined ‘series of questions’ that determines if a shutdown is necessary; and (3) any executing protocols or guidelines related to the implementation of SOP 303, distributed to DHS, other federal agencies, or private companies, including protocols related to oversight of shutdown determinations.” Id., ¶ 9. DHS responded to EPIC on August 21, 2012, saying that it “had conducted comprehensive searches for records that would be responsive to the request[, but] . . . that [DHS was] unable to locate or identify any responsive records.” Id., ¶ 16. EPIC administratively appealed on October 2, 2012, and on March 25, 2013, the United States Coast Guard, Office of the Chief Administrative Law Judge – the office that reviews these FOIA appeals – “remanded the matter back to DHS Privacy for further review.” Id., ¶¶ 17-18.

Upon additional inspection, DHS located one responsive record, the very document EPIC had requested: Standard Operating Procedure 303. Id., ¶¶ 19-20. “Included as part of SOP 303 itself are the two other categories of records that EPIC seeks, *i.e.*, the full text of the pre-determined series of questions that determines if a shutdown is necessary, and the executing protocols related to the implementation of SOP 303.” Id., ¶ 21. DHS “determined that the SOP

is the only responsive document because there are no other documents that contain the full text of the questions or any executing protocols.” Id.

Portions of SOP 303 – “names, direct-dial telephone numbers, and email addresses for state homeland security officials” – were withheld from EPIC under Exemptions 6 and 7(C), which generally permit withholding of personal information. Id., ¶¶ 23-24. The remainder of the document was withheld under Exemptions 7(E) and 7(F), which permit withholding of certain law-enforcement information if it, respectively, would “disclose techniques and procedures for law enforcement investigations or prosecutions” or “could reasonably be expected to endanger the life or physical safety of any individual.” 5 U.S.C. § 552(b)(7); Holzer Decl., ¶¶ 25-26.

On February 27, 2013, EPIC filed this lawsuit seeking the release of the withheld portions of SOP 303. Both parties have now cross-moved for summary judgment.

II. Legal Standard

Summary judgment may be granted if “the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law.” Fed. R. Civ. P. 56(a). A genuine issue of material fact is one that would change the outcome of the litigation. See Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 248 (1986) (“Only disputes over facts that might affect the outcome of the suit under the governing law will properly preclude the entry of summary judgment.”). In the event of conflicting evidence on a material issue, the Court is to construe the evidence in the light most favorable to the non-moving party. See Sample v. Bureau of Prisons, 466 F.3d 1086, 1087 (D.C. Cir. 2006). Factual assertions in the moving party’s affidavits or declarations may be accepted as true unless the opposing party submits his own

affidavits, declarations, or documentary evidence to the contrary. Neal v. Kelly, 963 F.2d 453, 456 (D.C. Cir. 1992).

FOIA cases typically and appropriately are decided on motions for summary judgment. See Defenders of Wildlife v. Border Patrol, 623 F. Supp. 2d 83, 87 (D.D.C. 2009); Bigwood v. U.S. Agency for Int'l Dev., 484 F. Supp. 2d 68, 73 (D.D.C. 2007). In FOIA cases, the agency bears the ultimate burden of proof. See U.S. Dep't of Justice v. Tax Analysts, 492 U.S. 136, 142, n.3 (1989). The Court may grant summary judgment based solely on information provided in an agency's affidavits or declarations when they describe "the documents and the justifications for nondisclosure with reasonably specific detail, demonstrate that the information withheld logically falls within the claimed exemption, and are not controverted by either contrary evidence in the record nor by evidence of agency bad faith." Military Audit Project v. Casey, 656 F.2d 724, 738 (D.C. Cir. 1981). Such affidavits or declarations are accorded "a presumption of good faith, which cannot be rebutted by 'purely speculative claims about the existence and discoverability of other documents.'" SafeCard Servs., Inc. v. SEC, 926 F.2d 1197, 1200 (D.C. Cir. 1991) (quoting Ground Saucer Watch, Inc. v. CIA, 692 F.2d 770, 771 (D.C. Cir. 1981)).

III. Analysis

Congress enacted FOIA in order to "pierce the veil of administrative secrecy and to open agency action to the light of public scrutiny." Dep't of Air Force v. Rose, 425 U.S. 352, 361 (1976) (citation omitted). "The basic purpose of 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." John Doe Agency v. John Doe Corp., 493 U.S. 146, 152 (1989) (citation omitted). The statute provides that "each agency, upon any request for records which (i) reasonably describes such records and (ii) is made in accordance with

published rules . . . shall make the records promptly available to any person.” 5 U.S.C. § 552(a)(3)(A). Consistent with this statutory mandate, federal courts have jurisdiction to order the production of records that an agency improperly withholds. See 5 U.S.C. § 552(a)(4)(B); Dep’t of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 755 (1989). “Unlike the review of other agency action that must be upheld if supported by substantial evidence and not arbitrary and capricious, FOIA expressly places the burden ‘on the agency to sustain its action’ and directs the district courts to ‘determine the matter de novo.’” Reporters Comm., 489 U.S. at 755 (quoting 5 U.S.C. § 552(a)(4)(B)). “At all times courts must bear in mind that FOIA mandates a ‘strong presumption in favor of disclosure’” Nat’l Ass’n of Home Builders v. Norton, 309 F.3d 26, 32 (D.C. Cir. 2002) (quoting Dep’t of State v. Ray, 502 U.S. 164, 173 (1991)).

In moving for summary judgment, DHS first contends that its search was adequate. EPIC does not contest this point. DHS next maintains that its withholding of personal identifying information under Exemptions 6 and 7(C) was appropriate. EPIC makes no challenge here either. See Opp. at 5 n.1. Instead, it saves its ammunition for DHS’s claim that it properly withheld the bulk of SOP 303 under both Exemption 7(E) and 7(F). Because the Court ultimately finds that the agency’s invocation of these exemptions was not proper, it need not address the last issue EPIC raises – namely, whether DHS performed an appropriate segregability analysis. The Court will begin with a discussion of 7(E) and then move to a consideration of 7(F).

A. Exemption 7(E)

Exemption 7 authorizes the Government to withhold “records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement

records or information” meets one of six requirements. 5 U.S.C. § 552(b)(7); see Keys v. Dep’t of Justice, 830 F.2d 337, 340 (D.C. Cir. 1987) (“[Exemption 7] exempts such documents from disclosure only to the extent that production of the information might be expected to produce one of six specified harms.”). The fifth subparagraph – 7(E) – permits withholding where production “would disclose techniques and procedures for law enforcement investigations or prosecutions.” 5 U.S.C. § 552(b)(7)(E). The agency here must thus satisfy two requirements: First, the record must be compiled for law-enforcement purposes; and second, production must disclose techniques and procedures for law-enforcement investigations.

DHS clearly surpasses the first hurdle. “Steps by law enforcement officers to prevent terrorism surely fulfill ‘law enforcement purposes.’” Milner v. Dep’t of Navy, 131 S. Ct. 1259, 1272 (2011) (Alito, J., concurring). DHS need only make “a colorable claim” of a rational nexus “between the agency’s activity [that created the document] and its law enforcement duties.” Keys, 830 F.2d at 340. DHS created SOP 303 to “establish[] a protocol for verifying that circumstances exist that would justify shutting down wireless networks” “to efficiently and effectively deter the triggering of radio-activated improvised explosive devices.” Holzer Decl., ¶ 25. There is, accordingly, a rational nexus between SOP 303’s protocol for preventing the triggering of radio-activated IEDs and DHS’s law-enforcement purpose of keeping the country safe.

DHS’s trouble comes at the second step, which requires that the disclosure would reveal “techniques and procedures for law enforcement investigations or prosecutions.” 5 U.S.C. § 552(b)(7)(E). The key question is whether the agency has sufficiently demonstrated how SOP 303, which articulates protective measures, is a technique or procedure “for law enforcement investigations or prosecutions.” Id.

The Court must begin by “presum[ing] that a legislature says in a statute what it means and means in a statute what it says there.” Connecticut Nat’l Bank v. Germain, 503 U.S. 249, 253-54 (1992). Of particular relevance here, Congress amended FOIA in 1986. See PL 99-570, Oct. 27, 1986, 100 Stat 3207. Prior to the 1986 amendments, to merit withholding, Exemption 7 first required “investigatory records compiled for law enforcement purposes,” and subparagraph (E) then required that the records would “disclose investigative techniques and procedures.” See PL 93-502, Nov. 21, 1974, 88 Stat 1561. The 1986 amendments “delet[ed] any requirement [in the first step] that the information be ‘investigatory,’” Tax Analysts, 294 F.3d at 79, and broadened the permissible withholding to “records or information compiled for law enforcement purposes.” See PL 99-570, Oct. 27, 1986, 100 Stat 3207. Congress, however, retained the investigatory requirement in 7(E). See id. (slightly modifying subparagraph (E), but keeping requirement that information be “for law enforcement investigations or prosecutions”). Congress thus specifically and intentionally chose to remove the investigatory requirement from the first step and to leave it in the second step. The Court, therefore, will apply “the usual rule that ‘when the legislature uses certain language in one part of the statute and different language in another, the court assumes different meanings were intended.’” Sosa v. Alvarez-Machain, 542 U.S. 692, 711 n.9 (2004) (quoting 2A N. Singer, Statutes and Statutory Construction § 46:06, p. 194 (6th rev. ed. 2000)).

Looking at the amended language, the Court agrees with the Government that Exemption 7’s mention of “law enforcement purposes” may certainly include preventive measures. See Mot. at 9-10. The problem is that 7(E)’s reference to “law enforcement investigations and prosecutions” does not. This distinction finds support in Justice Alito’s concurrence in Milner, a case that dealt with the applicability of Exemption 2. In his opinion, Justice Alito explained that

“[t]he ordinary understanding of law enforcement [purposes] includes not just the investigation and prosecution of offenses that have already been committed, but also proactive steps designed to prevent criminal activity and to maintain security.” Milner, 131 S. Ct. at 1272 (Alito, J., concurring). Justice Alito went on to explain how, in context, Exemption 7’s reference to “law enforcement purposes” “involve[s] more than just investigation and prosecution,” which he describes as “narrower activities” confined to Exemption 7’s subparagraphs. See id. at 1273 (“Congress’ decision to use different language to trigger Exemption 7 confirms that the concept of ‘law enforcement purposes’ sweeps in activities beyond [subparagraph (E)’s] investigation and prosecution.”)

If “techniques and procedures for law enforcement investigations or prosecutions” is given its natural meaning, it cannot encompass the protective measures discussed in SOP 303. This term refers only to acts by law enforcement after or during the commission of a crime, not crime-prevention techniques. Reading Exemption 7(E) as such, moreover, is in keeping with FOIA’s “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) (internal quotation marks omitted), and the well-settled practice of reading FOIA exemptions narrowly. See Milner, 131 S. Ct. at 1265 (“We have often noted ‘the Act’s goal of broad disclosure’ and insisted that the exemptions be ‘given a narrow compass.’”) (quoting Dep’t of Justice v. Tax Analysts, 492 U.S. 136, 151 (1989)).

In arguing against such an interpretation, DHS relies on a nearly 30-year-old case from this district that upheld the Secret Service’s invocation of Exemption 7(E) to shield “records pertaining to . . . two armored limousines for the President.” U.S. News & World Report v. Dep’t of Treasury, 1986 U.S. Dist. LEXIS 27634, at *1 (D.D.C. March 26, 1986). In that case,

the court rejected plaintiff's argument – similar to the one EPIC makes here – “that the information at issue [] would reveal ‘protective’ not ‘investigative’ techniques and procedures” and concluded that “[i]t is inconceivable . . . that Congress meant to afford these [preventive] activities any less protection from disclosure simply because they do not fit within the traditional notion of investigative law enforcement techniques.” *Id.* at *6. This case, however, was decided before the 1986 amendments changed the language of the relevant clauses, making it not “inconceivable,” but in fact probable that Congress intended to differentiate between preventive and investigative activities. *U.S. News* also predates *Milner*'s insistence on reading the exemptions narrowly. *See* 131 S. Ct. at 1265; *see also Dep't of Justice v. Landano*, 508 U.S. 165, 181 (1993) (noting Court's “obligation to construe FOIA exemptions narrowly in favor of disclosure”). The Court, therefore, does not believe *U.S. News* dictates a different result.

The agency's last gambit is a *post hoc* attempt in its Reply to classify SOP 303 as an investigative technique. It claims that “[p]reventing explosives from detonating preserves evidence . . . and, thereby, facilitates the investigation into who built and placed the bomb.” *See* Def's Reply at 5-6. This is too little, too late. As EPIC notes, “[N]o ordinary speaker of the English language” would describe SOP 303 – “a protocol for verifying that circumstances exist that would justify shutting down wireless networks” “to efficiently and effectively deter the triggering of radio-activated improvised explosive devices,” Holzer Decl., ¶ 25 – as an evidence-gathering technique. Pl's Reply at 3.

The Court will thus read Exemption 7(E) in a manner that harmonizes with FOIA's purpose of disclosure, the canons of statutory construction, and the Supreme Court's guidance to read FOIA's exemptions narrowly.

B. Exemption 7(F)

DHS next argues that SOP 303 was also properly withheld under Exemption 7(F). This exemption authorizes the Government to withhold “records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information . . . could reasonably be expected to endanger the life or physical safety of any individual.” 5 U.S.C. § 552(b)(7)(F). As the Court explained in relation to Exemption 7(E), the agency easily clears the “law enforcement purposes” hurdle. See Section III.A, *supra*.

Yet again, though, the second requirement leads to DHS’s undoing. DHS must show that production would “endanger the life or physical safety of any individual.” 5 U.S.C. § 552(b)(7)(F) (emphasis added). The agency argues that SOP 303’s “disclosure could reasonably be expected to endanger the physical safety of individuals near unexploded bombs.” Mot. at 13. DHS’s thinking goes like this: 1) SOP 303 “describes a procedure for shutting down wireless networks to prevent bombings”; 2) “[r]eleasing information regarding this protocol would enable ‘bad actors’ to blunt its usefulness”; and 3) this “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.” Id. In other words, the “any individual” test is satisfied because those endangered are any individuals near a bomb. Although this interpretation holds some appeal, the Court must conclude that the agency reads the “any individual” standard too broadly.

While DHS is correct that Exemption 7(F) is not limited to protecting law-enforcement personnel from harm, see Amuso v. Dep’t of Justice, 600 F. Supp. 2d 78, 101 (D.D.C. 2009), the agency still must identify the individuals at risk with some degree of specificity. See ACLU v. Dep’t of Defense, 543 F.3d 59, 66-72 (2d Cir. 2008) (“The phrase ‘any individual’ in exemption 7(F) may be flexible, but is not vacuous.”), vacated on other grounds, 558 U.S. 1042 (2009).

The Second Circuit in ACLU considered a similar question to the one raised here, and its opinion is instructive. The Government there wished to apply the “any individual” standard to prevent the release of photographs “depict[ing] abusive treatment of detainees by United States soldiers in Iraq and Afghanistan” on the ground that “the release of the disputed photographs will endanger United States troops, other Coalition forces, and civilians in Iraq and Afghanistan.” Id. at 63. In an extensive examination of the phrase “any individual” – in light of the Supreme Court’s admonition to interpret FOIA exemptions narrowly – the court rejected the Government’s argument “that it could reasonably be expected that out of a population the size of two nations and two international expeditionary forces combined, someone somewhere will be endangered as a result of the release of the Army photos.” Id. at 71. It concluded that “an agency must identify at least one individual with reasonable specificity and establish that disclosure of the documents could reasonably be expected to endanger that individual.” Id.

Central to the ACLU court’s holding was its thorough examination of the legislative history of 7(F), which this Court also finds significant. Prior to the 1986 FOIA amendments, Exemption 7(F) protected records, the release of which would “endanger the life or physical safety of law enforcement personnel.” See PL 93-502, Nov. 21, 1974, 88 Stat 1561 (emphasis added). The exemption served to withhold “information which would reveal the identity of undercover agents, State or Federal, working on such matters as narcotics, organized crime, terrorism, or espionage.” Edward A. Levi, Attorney General’s Memorandum on the 1974 Amendments to the Freedom of Information Act, pt. I.B (1975), available at <http://www.justice.gov/oip/74agmemo.htm>, cited in ACLU, 543 F.3d at 77-78. The exemption did not cover witnesses, interviewees, victims, informants, or families of law-enforcement personnel; as a result, among other impairments, it “harmed the ability of law enforcement

officers to enlist informants.” Statement of the Chair of the Senate Committee on the Judiciary’s Subcommittee on the Constitution (the subcommittee with jurisdiction over FOIA), 131 Cong. Rec. S263 (daily ed. Jan. 3, 1985), cited in ACLU, 543 F.3d at 78.

To remedy this omission, the Government asked for an amendment to “modif[y] slightly – not revise[] wholesale” – the scope of 7(F). Statement of Carol E. Dinkins, Deputy Attorney General, 131 Cong. Rec. S263 (daily ed. Jan. 3, 1985), cited in ACLU, 543 F.3d at 79. As the Government stated in support of the amendment:

The current language in Exemption 7(F) exempts records only if their disclosure would endanger the life of a law enforcement officer. However, the exemption does not give similar protection to the life of any other person. [The proposed amendment] expands Exemption 7(F) to include such persons as witnesses, potential witnesses, and family members whose personal safety is of central importance to the law enforcement process.

Id., cited in ACLU, 543 F.3d at 78. Congress complied, passing “only modest changes to the FOIA . . . , [a]nd slight[ly] expan[ding] . . . exemption[] . . . (7)(F).” Statement of the Chair of the House Committee on Government Operations, Subcommittee on Government Information, Justice, and Agriculture (the subcommittee with jurisdiction over FOIA), 132 Cong. Rec. H9455 (daily ed. Oct. 8, 1986), cited in ACLU, 543 F.3d at 79.

Congress ultimately settled on the broader term of “any individual,” as opposed to, for example, “any individual connected to or assisting law enforcement.” The Court, therefore, would be overly restrictive if it defined “any individual” in the latter, cabined manner. Yet, bearing in mind the modest expansion intended and the prescription that exemptions must be read narrowly, the Court must require some specificity and some ability to identify the individuals endangered.

Against this backdrop, the Government here nonetheless seeks a broader interpretation of “any individual” than was rejected in ACLU. The individuals that DHS claims satisfy the standard are anyone “within the blast radius of a remotely detonated bomb.” See Def’s Mot. at 12-13; Def’s Reply at 11. As EPIC notes, “These hypothetical bombs” – like the hypothetical danger to troops and civilians in ACLU – “could materialize at any time, in any place, and affect anyone in the United States.” Pl’s Reply at 9. These individuals, therefore, are “identified only as a member of a vast population.” ACLU, 543 F.3d at 68. In fact, the population is vaster here because it encompasses all inhabitants of the United States, while in ACLU it only covered people in Iraq and Afghanistan. Indeed, if the Government’s interpretation were to hold, there is no limiting principle to prevent “any individual” from expanding beyond the roughly 300 million inhabitants of the United States, as the Government proposes here, to the seven billion inhabitants of the earth in other cases. This expansive interpretation of “any individual” is far broader than what the Government had in mind when it requested a “slight[]” enlargement of 7(F) in 1985, and far more than Congress approved in its “slight expansion of exemption[] . . . (7)(F)” in 1986. See 131 Cong. Rec. at S263; 132 Cong. Rec. at H9455.

The primary case DHS relies on for the proposition that anyone near unexploded bombs is a specific-enough group, Living Rivers, Inc. v. U.S. Bureau of Reclamation, 272 F. Supp. 2d 1313 (D. Utah 2003), is easily distinguishable. In that case, the court upheld the Government’s invocation of Exemption 7(F) to withhold inundation maps that showed downstream communities that would be at risk in the event of dam failure. Id. at 1315, 1321-22. The danger was that terrorists could use the maps to better plan prospective attacks. Id. at 1321. There is a critical difference, however, between the populations in danger in that case and this one. In Living Rivers, the Government contended that “disclosure of the inundation maps ‘could

reasonably place at risk the life or physical safety of those individuals who occupy the downstream areas that would be flooded by a breach of Hoover Dam or Glen Canyon Dam.”

Id. (emphasis added) (internal citation omitted). Here, the individuals at risk include anyone near any unexploded bomb, which could include anyone anywhere in the country. See Mot. at 12-13, Def’s Reply at 11. As the Living Rivers population was clearly specified and limited, the case, even were it binding, does not affect the Court’s decision.

The additional cases DHS cites in its Reply for the proposition that individuals need not be specifically identified all involve far narrower groups with readily identifiable members than those at risk here. See Zander v. Dep’t of Justice, 885 F. Supp. 2d 1, 7 (D.D.C. 2012) (upholding 7(F) withholding where Government identified class of people at risk as police officers working in prisons while forcibly removing prisoners from their cells); Pub. Employees for Envtl. Responsibility v. U.S. Section Int’l Boundary & Water Comm’n, 839 F. Supp. 2d 304, 327-28 (D.D.C. 2012) (upholding 7(F) withholding of inundation maps for similar reasons as those in Living Rivers); Peter S. Herrick’s Customs & Int’l Trade Newsletter v. U.S. Customs & Border Prot., No. 04-00377, 2006 WL 1826185, at *8-9 (D.D.C. June 30, 2006) (upholding 7(F) withholding relating to, *inter alia*, customs officials’ seized contraband because information’s release would “put[] Customs’ officials at risk from individuals who would seek to acquire such items”).

Reading 7(F) to encompass possible harm to anyone anywhere in the United States within the blast radius of a hypothetical unexploded bomb also flies in the face of repeated Supreme Court direction to read FOIA exemptions narrowly. See Milner, 131 S. Ct. at 1265 (“We have often noted ‘the Act’s goal of broad disclosure’ and insisted that the exemptions be ‘given a narrow compass.’”) (quoting Dep’t of Justice v. Tax Analysts, 492 U.S. 136, 151

(1989)); Landano, 508 U.S. at 181 (noting Court’s “obligation to construe FOIA exemptions narrowly in favor of disclosure”); Rose, 425 U.S. at 361 (noting “basic policy that disclosure, not secrecy, is the dominant objective of the Act”). Exemption 7(F), therefore, cannot be read as expansively as the Government proposes, and thus cannot justify withholding SOP 303. The Court does not dispute that it will be difficult in some cases to decide whether endangered individuals have been sufficiently identified, but such hardship does not exist here.

* * *

In reaching its conclusion, the Court is not unaware of the potential adverse use to which this information could be put. Its ruling, furthermore, is no judgment on whether it is in the national interest for SOP 303 to be disclosed. If, in fact, the Government believes release will cause significant harm, it has other options to pursue. As the Supreme Court explained in Milner, “If these or other exemptions do not cover records whose release would threaten the Nation’s vital interests, the Government may of course seek relief from Congress. . . . All we hold today is that Congress has not enacted the FOIA exemption the Government desires. We leave to Congress, as is appropriate, the question whether it should do so.” Milner, 131 S. Ct. at 1271. Indeed, in issuing guidance on FOIA exemptions in a post-Milner world, the Department of Justice’s Office of Information Policy concluded that “it seems inevitable that there will be some sensitive records that will not satisfy the standards of any of the Exemptions.” OIP Guidance, Exemption 2 After the Supreme Court’s Ruling in Milner v. Department of the Navy 15 available at <http://www.justice.gov/oip/foiapost/milner-navy.pdf>. Standard Operating Procedure 303 is such a record.

IV. Conclusion

For the foregoing reasons, the Court will issue a contemporaneous Order granting judgment in Plaintiff's favor and ordering DHS to turn over SOP 303 – with redactions related only to Exemptions 6 and 7(C) – to Plaintiff within 30 days. Mindful of the national-security implications involved, and appreciating that disclosure of SOP 303 would effectively moot any appeal, this Opinion and accompanying Order will be stayed for 30 days in order to allow for either appeal, should the Government wish to file one, or another type of cure – *e.g.*, classification of the document to exempt it from disclosure under Exemption 1 or legislation exempting it from FOIA under Exemption 3. If DHS notices an appeal by December 12, 2013, the stay shall remain in effect until the Court of Appeals rules on such appeal.

/s/ James E. Boasberg
JAMES E. BOASBERG
United States District Judge

Date: November 12, 2013

**IN THE 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.)	
_____)	

NOTICE OF APPEAL

NOTICE IS HEREBY GIVEN that Defendant, Department of Homeland Security, hereby appeals to the United States Court of Appeals for the District of Columbia Circuit from this Court's Order and this Court's Memorandum Opinion entered on November 12, 2013 (Docket Nos. 18, 19), which granted Plaintiff's motion for summary judgment and denied Defendant's motion for summary judgment.

Dated: January 13, 2014

Respectfully submitted,

STUART F. DELERY
Assistant Attorney General

RONALD C. MACHEN JR
United States Attorney

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

/s/ Justin M. Sandberg
JUSTIN M. SANDBERG

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

Attorneys for Defendant

CERTIFICATE OF SERVICE

I hereby certify that on June 4, 2014, I electronically filed the foregoing with the Clerk of the Court by using the appellate CM/ECF system.

/s/ Adam Jed

Adam C. Jed