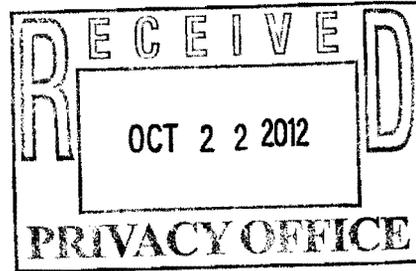


EXHIBIT 4

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.

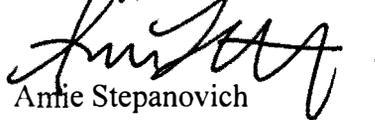
EPIC Renews Its Request for Expedited Treatment and Requests Expedited Treatment of this Appeal

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 riles privacy group*, Jaikumar Vijayan, Computerworld, July 10, 2012

http://www.computerworld.com/s/article/9228950/White_House_order_on_emergency_communications_riles_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>).

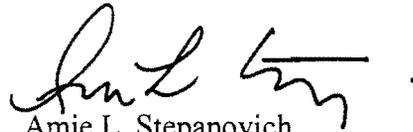
²⁸ See EPIC: EPIC v. Department of Homeland Security: Media Monitoring, <http://epic.org/foia/epic-v-dhs-media-monitoring/> (last visited July 9, 2012).

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

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



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

CERTIFIED MAIL™



7010 2780 0001 9823 5702



ELECTRONIC PRIVACY INFORMATION CENTER

epic.org

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

FOIA Appeal DHS/OS/PRIV 12-
0598

1-1

1-

485
Delivery Point

Bldg 1

associate general counsel

Processed By: DSS-990M-019
9/19/2012 11:18:01 AM



70102780000198235702