

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

ELECTRONIC PRIVACY INFORMATION CENTER)	
)	
Plaintiff,)	
)	
v.)	No. 1:12-cv-00333-GK
)	
THE UNITED STATES DEPARTMENT OF HOMELAND SECURITY)	
)	
Defendant.)	
)	

**PLAINTIFF’S OPPOSITION TO DEFENDANT’S MOTION FOR AN
ADDITIONAL 10-DAY STAY OF PROCEEDINGS**

Plaintiff the Electronic Privacy Information Center (“EPIC”) opposes Defendant U.S. Department of Homeland Security’s (“DHS”) September 5, 2012 Motion for a second 10-Day Stay of Proceedings. On March 24, 2012, this Court ordered the complete production of documents and a Vaughn index by August 24, 2012. The agency essentially ignored the deadline, waited until the last moment to begin the processing of the request, moved for a stay, sought EPIC’s agreement to narrow the scope of the request (which EPIC promptly agreed to), and now simply seeks more delay without a clear commitment to provide any documents responsive to the request.

This case arises from the July 26, 2011 EPIC Freedom of Information Act request to the DHS regarding the “DIB Pilot,” a joint program between DHS and the National Security Agency (“NSA”) to monitor Internet traffic (“EPIC’s FOIA Request”). The DIB Pilot raises substantial concerns about the privacy of Internet users and whether the

government may be ignoring the obligations of Internet Service Providers to comply with the Electronic Communications Privacy Act. Specifically, EPIC requested:

1. All contracts and communications with Lockheed Martin, CSC, SAIC, Northrop Gumman, or any other defense contractors regarding the new NSA pilot program;
2. All contracts and communications with AT&T, Verizon, and CenturyLink or any other ISPs regarding the new NSA pilot program;
3. All analyses, legal memoranda, and related records regarding the new NSA pilot program;
4. Any memoranda of understanding between NSA and DHS or any other government agencies or corporations regarding the new NSA pilot program.¹

More than seven months passed and the agency failed to make a determination on EPIC's FOIA Request. EPIC filed suit in this Court on March 1, 2012 to compel the Defendant to produce documents.

On May 21, 2012, as per the Court's order, the parties filed a Joint Meet and Confer Statement in which they agreed on all matters except the proposed schedule. EPIC proposed that the Court establish concrete deadlines for the production of documents and the filing of dispositive motions. EPIC further proposed that the Defendant complete document production and a Vaughn Index by August 24, 2012, with subsequent filings to follow on a set schedule. The Defendant proposed instead to conduct the search in two stages. DHS proposed to first identify documents that are potentially responsive to the EPIC FOIA Request within "approximately six weeks," or by around June 27, 2012. The Defendant then proposed a second stage to review the documents and consult with other

¹ EPIC's FOIA Request additionally requested a fifth category of documents, "any privacy impact assessment performed as part of the development of the new NSA pilot program." On August 3, 2011, in DHS' acknowledgement of EPIC's FOIA Request, DHS notified EPIC that a search had been performed and DHS had been unable to identify or locate any records that were responsive to this fifth category of documents.

agencies. The DHS stated, “DHS proposes that it will make its first production by July 18, 2012.”

On March 24, 2012, upon consideration of the parties Joint Meet and Confer Statement, this Court set out a Scheduling Order that required Defendant’s Complete Production of Documents and Vaughn Index by August 24, 2012.

On August 24, 2012, the date documents were due, the Defendant contacted EPIC for the first time since the Court entered the Scheduling Order.² The Defendant then filed a Motion for a 10-day stay of proceedings, which this Court granted on August 27, 2012.³

Defendant then waited almost a week to contact EPIC at which time counsel stated that the “vast majority” and the “broadest category” of records potentially responsive to the EPIC FOIA request were in the category “all analyses, legal memoranda, and related records regarding the [DIB Cyber Pilot].” EPIC promptly agreed to narrow the scope of the request, asking simply for “all legal and technical analyses, including legal memoranda, regarding the DIB cyber pilot.”

A stay is appropriate in a Freedom of Information Act case in “exceptional circumstances,” 5 U.S.C. § 552(a)(6)(C), when a demonstration is made that the agency “has limited resources, is deluged with volume of requests for information vastly in excess of that anticipated by Congress, and is exercising due diligence in processing request.” *Edmond v. US Atty*, 959 F.Supp. 1, 2-3 (D.D.C. 1997), citing *Open America v. Watergate Special Prosecution Force*, 547 F.2d 605, 614-16 (D.C. Cir. 1976) Defendant

² Email from Lisa Marcus, Trial Attorney, U.S. Department of Justice to Amie Stepanovich, Associate Litigation Counsel, EPIC (Aug. 24, 2012) (on file with EPIC).

³ At this time, over thirteen months have passed since DHS received EPIC’s FOIA Request, nearly six months have passed since EPIC filed the lawsuit, the scheduling order was adopted five months ago, and DHS represented that the agency could complete a search for documents over two months ago.

has not alleged any of these circumstances. Moreover, defendant should not wait until the ultimate deadline for the production of documents to begin communications with the requester about the scope of the request. Such a tactic encourages delay.

The timely release of documents sought in this matter is both important and necessary. The Department of Justice (“DOJ”) has expressed misgivings that the program that is the subject of EPIC’s FOIA Request could “run afoul of privacy laws forbidding government surveillance of private Internet traffic.”⁴ And Congress is currently engaged in a high-profile debate over cybersecurity, the role of government, and the privacy of Internet users. The documents sought by EPIC in this matter lie at the epicenter of this policy debate.⁵

⁵ See, e.g., Cyber Intelligence Sharing and Protection Act of 2011, H.R. 3523, 112th Cong. (2012) (Passed by House on April 26, 2012), available at <http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/HR3523.pdf>; Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology (“SECURE IT”) Act of 2012, S. 2151, 112th Cong. (2012), available at [http://thomas.loc.gov/cgi-bin/bdquery/z?d112:s.2151](http://thomas.loc.gov/cgi-bin/bdquery/z?d112:s.2151;); The Cybersecurity Act of 2012, S. 2105, 112th Cong. (2012), available at <http://thomas.loc.gov/cgi-bin/query/z?c112:S.2105>. A robust debate followed each of these bills, and privacy experts, along with members of the public, acknowledged many fundamental flaws. See, e.g., *Cybersecurity at Risk*, N.Y. Times (July 31, 2012), <http://www.nytimes.com/2012/08/01/opinion/cybersecurity-at-risk.html>; Ellen Nakashima, *Cybersecurity Bill Poised for Senate Consideration*, Wash. Post (July 24, 2012), http://www.washingtonpost.com/world/national-security/cybersecurity-bill-poised-for-senate-consideration/2012/07/24/gJQAZxpU7W_story.html; Siobhan Gorman, *Cybersecurity Bill Blocked as Hopes Dim for Compromise*, Wall St. J. (Aug. 2, 2012), <http://online.wsj.com/article/SB10000872396390443866404577565121771512102.html>. As the legislative debate has raged, President Obama has sought to utilize his executive authority to implement cybersecurity measures. See Carlo Munoz, *White House Considers Executive Action to Address Cybersecurity*, The Hill (Aug. 8, 2012), <http://thehill.com/blogs/defcon-hill/policy-and-strategy/242799-white-house-considers-executive-action-to-address-cybersecurity-threats->; Eric Engleman, *Obama Considering Executive Branch Action on Cybersecurity*, Bloomberg BusinessWeek (Aug. 8, 2012), <http://www.businessweek.com/news/2012-08-08/obama-considering-executive-branch-action-on-cybersecurity-plan>; Eamon Javers, *Obama’s Internet Order: Power Grab or Simple Update*, CNBC (July 11, 2012), http://www.cnbc.com/id/48151460/Obama_s_Internet_Order_Power_Grab_or_Simple_Update. The Defendant, DHS, has also moved forward independently on issues of cybersecurity. See DHS, *Public and Private Sector Experts Gather in Atlanta to Strengthen Partnerships and Address Cyber Threats*, <http://www.dhs.gov/blog/2012/08/27/strengthening-partnerships-and-addressing-cyber-threats> (last visited Sept. 4, 2012).

As the D.C. Circuit has recognized, “an understanding of how [a federal agency] makes policy decisions...is important to the public’s understanding of the government.” *Judicial Watch v. Rossotti*, 326 F.3d 1309, 1313–14 (D.C. Cir. 2003)). The records responsive to EPIC’s FOIA Request are vital to public understanding of the government’s cybersecurity efforts.

Despite this Court’s order and the Defendant’s representation that it could identify responsive documents by June 27, 2012 and produce documents by July 18, 2012, the Defendant has not yet produced a single document. Defendant now seeks a second stay but has failed to provide a date certain by which time any documents might actually be produced.

The Defendant has delayed these proceedings unnecessarily and appears set to continue on its current course. EPIC has agreed to significantly narrow the scope of its FOIA Request so that the agency may comply with the Scheduling Order. Accordingly, EPIC now respectfully asks the Court to deny Defendant’s motion for a second 10-day stay of these proceedings.

Respectfully submitted,

MARC ROTENBERG
GINGER McCALL
AMIE STEPANOVICH*
Electronic Privacy Information Center
1718 Connecticut Ave., NW
Suite 200
Washington, D.C. 20009
(202) 483-1140
Counsel for Plaintiff

* Amie Stepanovich is barred in New York State. Her application for admission in the District of Columbia is pending.