



July 26, 2011

VIA FACSIMILE: (703) 235-0443

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

Dear Ms. Callahan:

This letter constitutes a request under the Freedom of Information Act (“FOIA”), 5 U.S.C. § 552, and is submitted on behalf of the Electronic Privacy Information Center (“EPIC”). EPIC seeks documents regarding a joint National Security Agency (“NSA”) and Department of Homeland Security (“DHS”) pilot program, which has not been publicly named, designed to monitor all internet traffic routed to several defense contractors and attempts to detect whether there are malicious programs within this internet traffic designed to compromise the defense contractor security.

### Background

The Washington Post reported on June 16, 2011 that the NSA implemented a new program in May designed to monitor all traffic flowing through certain ISPs to a select number of defense contractors.<sup>1</sup> The current purported goal of this pilot program is the “thwarting [of] cyberattacks against defense firms,” although Deputy Secretary of Defense William J. Lynn III stated that “[w]e hope the . . . cyber pilot can be the beginning something bigger.”<sup>2</sup> According to Lynn, the NSA pilot program is to serve as a model that can be “transported to other critical infrastructure sectors, under the leadership of the Department of Homeland Security.”<sup>3</sup>

In the week after this program became public knowledge, the Washington Post and the Atlantic<sup>4</sup> provided any press coverage. Although no public name has been given to this new program, it is known that the NSA has partnered with ISPs AT&T, Verizon

<sup>1</sup> *NSA Allies with Internet Carriers to Thwart Cyber Attacks Against Defense Firms*, Ellen Nakashima, WASH. POST, June 16, 2011 [http://www.washingtonpost.com/national/major-internet-service-providers-cooperating-with-nsa-on-monitoring-traffic/2011/06/07/AG2dukXH\\_story.html](http://www.washingtonpost.com/national/major-internet-service-providers-cooperating-with-nsa-on-monitoring-traffic/2011/06/07/AG2dukXH_story.html).

<sup>2</sup> *Id.*

<sup>3</sup> *Id.*

<sup>4</sup> *See Prepare to Have Your Email Read by the NSA*, Adam Estes, THE ATLANTIC, June 17, 2011 <http://www.theatlanticwire.com/technology/2011/06/prepare-have-your-email-read-nsa/38931/>. Despite the provocative headline, none of the details offered in the article suggest that the NSA is actually reading e-mails (at least as part of this new program).

and CenturyLink to filter the traffic of fifteen defense contractors, including Lockheed Martin, CSC, SAIC and Northrop Grumman. The NSA claims that it will not be “direct[ly] monitoring the contractors’ networks”; instead, it has developed “signatures” of malicious code as well as sequences of suspicious network behavior that it will apply to filter all internet traffic on those ISPs that is “flowing” to these defense contractors.<sup>5</sup> By applying these signatures and filtering suspicious behavior, the NSA will be able to “disable the threats before an attack can penetrate a contractor’s servers.”<sup>6</sup>

Individuals within the Department of Justice (“DOJ”), likely in the Office of Legal Counsel (“OLC”), which provides opinions on the legality of executive branch programs, reportedly expressed misgivings that the program would “run afoul of privacy laws forbidding government surveillance of private Internet traffic.”<sup>7</sup> Presumably this refers to the Electronic Communications Privacy Act (“ECPA”), codified at 18 U.S.C. § 2510, which prohibits the interception of electronic communications without a court order or consent from one of the parties. However, the NSA has reportedly “allayed that concern by saying that the government will not directly filter the traffic or receive the malicious code captured by Internet providers.”<sup>8</sup> It is unclear how the program can detect “malicious code” and prevent its execution without “captur[ing]” it in violation of federal law, but Lynn may be offering some explanation by stating that the “threat intelligence provided by the government is helping the companies themselves, or the Internet service providers working on their behalf, to identify and stop malicious activity within their networks.”<sup>9</sup>

Deputy Secretary of Defense William J. Lynn III publicly spoke about the program and provided a rough outline of its scope.<sup>10</sup> He stated that it is currently run by the NSA, and that DHS is a partner.

#### Requested Documents

1. All contracts and communications with Lockheed Martin, CSC, SAIC, Northrop Grumman 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.

---

<sup>5</sup> See Nakashima, *supra* note 1.

<sup>6</sup> *Id.*

<sup>7</sup> *Id.*

<sup>8</sup> *Id.*

<sup>9</sup> *Id.*

<sup>10</sup> See Nakashima, *supra* note 1.

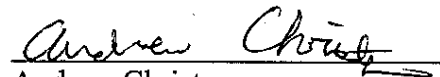
5. Any privacy impact assessment performed as part of the development of the new NSA pilot program.

Request for "News Media" Fee Status

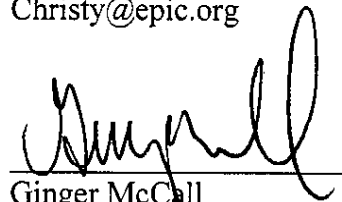
EPIC is a "representative of the news media" for fee waiver purposes. *EPIC v. Department of Defense*, 241 F. Supp. 2d 6 (D.D.C. 2003). Based on our status as a "news media" requester, we are entitled to receive the requested record with only duplication fees asserted. Further, because disclosure of this information will "contribute greatly public understanding of the operation or activities of the government," and duplication fees should be waived.

Thank you for your consideration of this request. As 5 U.S.C. § 552(a)(6)(E)(ii)(I) provides, I will anticipate your determination on our request within ten (10) calendar days.

Respectfully submitted,



Andrew Christy  
Law Clerk, EPIC  
Christy@epic.org



Ginger McCall  
Staff Counsel, EPIC  
Mccall@epic.org