



November 14, 2012

**VIA FACSIMILE (443)-479-3612**

National Security Agency  
ATTN: FOIA/PA Office (DJ4)  
9800 Savage Road, Suite 6248  
Ft. George G. Meade, MD 20755-6248

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.<sup>1</sup> This request is submitted on behalf of the Electronic Privacy Information Center (“EPIC”) to the National Security Agency (“NSA”). EPIC requests the public release of Presidential Policy Directive 20.

Background

On November 14, 2012, the Washington Post reported President Obama had signed Presidential Policy Directive 20 (“PPD 20”) in October.<sup>2</sup> According to the Washington Post, the Directive “enables the military to act more aggressively to thwart cyberattacks on the nation’s web of government and private computer networks.”<sup>3</sup> The text of the Directive has not been made public.<sup>4</sup>

The Washington Post reported that previous attempts at a Presidential Directive to expand the military’s cybersecurity authority had been dismissed as posing “unacceptable

<sup>1</sup> 5 U.S.C. § 552 (2011).

<sup>2</sup> Ellen Nakashima, *Obama signs secret cybersecurity directive, allowing more aggressive military role*, Washington Post (Nov. 14, 2012), [http://www.washingtonpost.com/world/national-security/obama-signs-secret-cybersecurity-directive-allowing-more-aggressive-military-role/2012/11/14/7bf51512-2cde-11e2-9ac2-1c61452669c3\\_story.html](http://www.washingtonpost.com/world/national-security/obama-signs-secret-cybersecurity-directive-allowing-more-aggressive-military-role/2012/11/14/7bf51512-2cde-11e2-9ac2-1c61452669c3_story.html); see also Carlos Munoz, *Report: Obama authorizes new cyber warfare directive*, The Hill (Nov. 14, 2012), <http://thehill.com/blogs/defcon-hill/policy-and-strategy/267879-report-obama-authorizes-new-cyber-warfare-directive>; Mathew J. Schwartz, *Obama Secret Order Authorizes Cybersecurity Strikebacks*, Information Week (Nov. 14, 2012), <http://www.informationweek.com/government/security/obama-secret-order-authorizes-cybersecur/240134945>; Charles Dharapak, *Obama Directive Would Allow Preemptive Cyber Strikes*, NextGov (Nov. 14, 2012), <http://www.nextgov.com/defense/2012/11/obama-directive-would-allow-preemptive-cyber-strikes/59522/>; Andrea Peterson, *Obama Signed Secret Directive to Thwart Cyberattack in Mid-October*, Think Progress (Nov. 14, 2012), <http://thinkprogress.org/security/2012/11/14/1189311/obama-signed-secret-directive-to-thwart-cyberattacks-in-mid-october/?mobile=nc>.

<sup>3</sup> *Obama signs secret cybersecurity directive, allowing more aggressive military role*, supra n. 2.

<sup>4</sup> *Id.*

risks” of “harmful unintended consequence[s].”<sup>5</sup> In addition, PPD 20 may violate federal law that prohibits military deployment within the United States without congressional approval.<sup>6</sup> The Washington Post reports that, following the issuance of PPD 20, the Pentagon is “expected to finalize new rules of engagement that would guide commanders when and how the military can go outside government networks to prevent a cyberattack that could cause significant destruction or casualties.”<sup>7</sup>

In 2008, President Bush issued National Security President Directive 54 (“NSPD 54”), which defined the cybersecurity authority of the National Security Agency. Despite a FOIA lawsuit filed by EPIC in 2009, that Directive has remained secret.<sup>8</sup> Since the issuance of NSPD 54, the NSA has been directly involved with the development of cybersecurity policy. EPIC noted that NSPD 54 is equivalent to “secret law,” the very thing the FOIA seeks to prevent.<sup>9</sup>

Transparency in cybersecurity is crucial to the public’s ability to monitor the government’s national security efforts and ensure that federal agencies respect privacy rights and comply with their obligations under the Privacy Act.<sup>10</sup> EPIC has previously testified to Congress on the need for privacy protections in cybersecurity efforts.<sup>11</sup> EPIC has also provided extensive comments under the Administrative Procedure Act to both the Department of Homeland Security and the Department of Defense on agency cybersecurity programs.<sup>12</sup> EPIC’s pursuit of NSPD 54 under the Freedom of Information Act has specifically challenged the NSA’s ability to promulgate secret cybersecurity laws.<sup>13</sup>

---

<sup>5</sup> *Id.*

<sup>6</sup> See 18 U.S.C. § 1385 (2012) Use of Army and Air Force as Posse Comitatus, available at [http://www.northcom.mil/About/history\\_education/posse.html](http://www.northcom.mil/About/history_education/posse.html); see also 10 U.S.C. § 375 (2012).

<sup>7</sup> *Obama signs secret cybersecurity directive, allowing more aggressive military role, supra* n. 2.

<sup>8</sup> EPIC: EPIC v. NSA – Cybersecurity Authority, [http://www.epic.org/privacy/nsa/epic\\_v\\_nsa.html](http://www.epic.org/privacy/nsa/epic_v_nsa.html) (last visited Nov. 14, 2012).

<sup>9</sup> Appellant’s Cross-Motion for Summary Judgment, Dkt. No. 14 at 16, *EPIC v. NSA*, (No. 10-00196); See also *NLRB v. Sears, Roebuck & Co.*, 421 U.S. 132, 137-138 (1975).

<sup>10</sup> See *EPIC v. NSA*, 678 F.3d 926 (D.C. Cir. 2012); EPIC: Cybersecurity Privacy Practical Implications, <http://www.epic.org/privacy/cybersecurity>; EPIC: EPIC v. NSA – Cybersecurity Authority, [http://www.epic.org/privacy/nsa/epic\\_v\\_nsa.html](http://www.epic.org/privacy/nsa/epic_v_nsa.html) (last visited Nov. 14, 2012); Memorandum, Dkt. No. 9, *EPIC v. NSA* (No. 10-00196).

<sup>11</sup> *Cybersecurity and Data Protection in the Financial Sector: Hearing Before the Subcomm. on Financial Institutions and Consumer Credit of the H. Comm. on Financial Services*, 112th Cong. (2011) (testimony and statement for the record of Marc Rotenberg, EPIC), available at <http://financialservices.house.gov/uploadedfiles/091411rotenberg.pdf>; *Cybersecurity and Data Protection in the Financial Sector: Hearing Before the S. Comm. on Banking, Housing, and Urban Affairs*, 112th Cong. (2011) (testimony and statement for the record of Marc Rotenberg, EPIC), available at [http://epic.org/privacy/testimony/EPIC\\_Senate\\_Banking\\_Testimony%206\\_21\\_11.pdf](http://epic.org/privacy/testimony/EPIC_Senate_Banking_Testimony%206_21_11.pdf).

<sup>12</sup> Comments of EPIC, DOD-2009-OS-0183/RIN 0790-AI60 (July 10, 2012), available at <http://epic.org/privacy/cybersecurity/EPIC-DOD-Cyber-Security-Comments.pdf>; Comments of EPIC, DHS-2010-0052 and DHS-2010-0053 (Dec. 15, 2010), available at [http://epic.org/privacy/fusion/EPIC\\_re\\_DHS-2010-0052\\_0053.pdf](http://epic.org/privacy/fusion/EPIC_re_DHS-2010-0052_0053.pdf).

<sup>13</sup> EPIC: EPIC v. NSA – Cybersecurity Authority, [http://www.epic.org/privacy/nsa/epic\\_v\\_nsa.html](http://www.epic.org/privacy/nsa/epic_v_nsa.html) (last visited Nov. 14, 2012); see also Letter from Jared Kaprove and John Verdi, EPIC to National Security Agency (Apr. 16, 2010), available at <http://epic.org/privacy/cybersecurity/EPIC-Ltr-Alexander-Supp-04-16-10.pdf> (requesting from the NSA the classified supplement to Lieutenant General Keith B. Alexander’s

## Documents Requested

Accordingly, EPIC requests the public release of Presidential Policy Directive 20.

## Request for News Media Fee Status

EPIC is a “representative of the news media” for FOIA purposes.<sup>14</sup> Based on our status as a “news media” requester, we are entitled to receive the requested records with only duplication fees assessed.<sup>15</sup> Further, because disclosure will “contribute significantly to public understanding of the operations or activities of the Department of Defense,” any duplication fees should be waived.<sup>16</sup> Consistent with the Department of Defense regulations, 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]’”.<sup>17</sup>

This FOIA request involves information on the National Security Agency’s authority to invade civilian Internet networks. Responsive documents will hold a great informative value regarding activities of the government 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.<sup>18</sup>

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 the Department of Justice (“DOJ”) for documents concerning the Bush-era warrantless wiretapping program.<sup>19</sup> EPIC’s request forced disclosure of two legal memos that provided new details on the program, including portions of the Bush Administration’s justification for

---

nomination hearings, including answers to questions about monitoring of private communications networks.).

<sup>14</sup> *EPIC v. Department of Defense*, 241 F.Supp.2d 5 (D.D.C. 2003).

<sup>15</sup> 32 C.F.R. § 286.28(e)(7) (2011), available at <http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=076b01743211e3fa64bf676e476d93e0&rgn=div8&view=text&node=32:2.1.1.2.66.6.1.1&idno=32>.

<sup>16</sup> 32 C.F.R. § 286.28(d).

<sup>17</sup> *Id.*

<sup>18</sup> See EPIC: EPIC Alert, <http://epic.org/alert/> (last visited Nov. 14, 2012).

<sup>19</sup> See EPIC: Freedom of Information Act Work on the National Security Agency's Warrantless Surveillance Program, <http://epic.org/privacy/nsa/foia/> (last visited Nov. 14, 2012).

the program.<sup>20</sup> EPIC was able to disseminate those documents to the public at large, which resulted in numerous news stories.<sup>21</sup>

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.<sup>22</sup> 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.

### 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."<sup>23</sup>

EPIC is "primarily engaged in disseminating information."<sup>24</sup>

There is a particular urgency for the public to obtain information about the NSA's cybersecurity activities within the United States. As previously discussed, numerous bills are currently being considered by Congress to address U.S. cybersecurity policy.<sup>25</sup> In order for meaningful public comment on these bills, as well as subsequent cybersecurity measures, the public must be aware of the authority that the President's Directive establishes.

In addition, the public has a further urgency to receive information about the NSA's authority to monitor domestic Internet networks. The NSA has an almost boundless capacity to intercept private communications.<sup>26</sup> The need to establish effective oversight for government surveillance, including matters involving national security, is well-understood and a long-standing concern.<sup>27</sup>

---

<sup>20</sup> *EPIC v. DOJ: Warrantless Wiretapping Memos Disclosed*, EPIC (Mar. 22, 2011), <http://epic.org/2011/03/epic-v-doj-warrentless-wiretap.html>.

<sup>21</sup> Josh Gerstein, *Justice Department details legal blessing of warrantless wiretapping in 2004*, Politico, March 19, 2011, [http://www.politico.com/blogs/joshgerstein/0311/Justice\\_Department\\_details\\_legal\\_blessing\\_of\\_warrantless\\_wiretapping\\_in\\_2004.html](http://www.politico.com/blogs/joshgerstein/0311/Justice_Department_details_legal_blessing_of_warrantless_wiretapping_in_2004.html) (describing the content of the memoranda released to EPIC and the ACLU); Dan Nguyen and Christopher Weaver, *The Missing Memos*, ProPublica, April 16, 2009, <http://www.propublica.org/special/missing-memos> (EPIC filed parallel lawsuits along with the ACLU lawsuits mentioned).

<sup>22</sup> EPIC: About EPIC, <http://epic.org/epic/about.html> (last visited Nov. 14, 2012).

<sup>23</sup> 5 U.S.C. § 552(a)(6)(E)(v)(II) (2008); *Al-Fayed v. CIA*, 254 F.3d 300, 306 (D.C. Cir. 2001).

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

<sup>25</sup> See *Cybersecurity Bills*, *supra* n. 5.

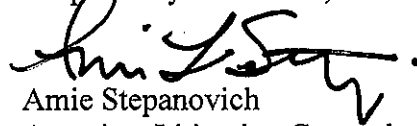
<sup>26</sup> Brief for EPIC et al. as Amici Curiae Supporting Petitioners at 18, *Clapper v. Amnesty International USA*, 638 F.3d 118 (2d Cir. 2011), *cert. granted* 566 U.S. 2 (May 21, 2012) (No. 11-1025).

<sup>27</sup> *Id.* at 30.

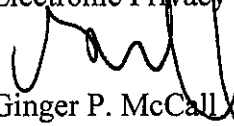
Conclusion

As provided in the FOIA, I will anticipate a determination within ten (10) calendar days. For questions regarding this request I can be contacted at 202-483-1140, ext. 104, or FOIA@epic.org.

Respectfully Submitted,



Amie Stepanovich  
Associate Litigation Counsel  
Electronic Privacy Information Center



Ginger P. McCall  
Director, Open Government Project  
Electronic Privacy Information Center