Aug. 4, 2009

VIA FACSIMILE (202-282-9186)
Office of the General Counsel (General Law)
Department of Homeland Security
Washington, DC 20528
Phone: 202-282-9822
Fax: 202-282-9186

RE: Freedom of Information Act Appeal and Renewed Request For Expedited Processing

Dear FOIA Appeals Officer:

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

On June 26, 2009, EPIC requested, *via* facsimile, documents regarding National Security Presidential Directive 54, otherwise referred to as The Homeland Security Presidential Directive 23 ("the Directive"). Specifically, EPIC requested:

1. The text of the National Security Presidential Directive 54, otherwise referred to as the Homeland Security Presidential Directive 23.

2. The full text, including previously unreported sections, of the Comprehensive National Cybersecurity Initiative, as well as any executing protocols distributed to the agencies in charge of its implementation.

3. All privacy policies related to either the Directive or the Comprehensive National Cybersecurity Initiative, including but not limited to, contracts or other documents describing privacy policies for information shared with private contractors to facilitate the Comprehensive National Cybersecurity Initiative.

See Appendix 1 ("EPIC's FOIA Request").

Factual Background

In January 2008, President George W. Bush issued the Directive, but it was never released to the public.[1] Under this Directive, the Comprehensive National Cybersecurity

[1] Jill R. Aitoro, *The Comprehensive National Cybersecurity Initiative*, NEXTGOV, June 1, 2009, http://www.nextgov.com/the_basics/tb_20090601_8569.php.

Initiative ("CNCI") was formed to "improve how the federal government protects sensitive information from hackers and nation states trying to break into agency networks."[2] In February 2009, President Obama appointed Melissa Hathaway as the head of a 60-day review of the government's cybersecurity efforts ("the Hathaway Report").[3] In April 2009, Senator Jay Rockefeller (D-WV) introduced to Congress the Cybersecurity Act of 2009 (S. 773), which is still pending in the Senate Committee on Commerce, Science, and Transportation.[4]

Despite a 2008 power struggle over the CNCI, the Department of Homeland Security ("DHS") was ultimately charged to oversee the details, with operational functions split between the National Security Agency (NSA), the Central Intelligence Agency (CIA), and the Federal Bureau of Investigation's (FBI) Cyber Division.[5] Each agency under DHS is responsible to "investigate intrusions by monitoring Internet activity and … capturing data for analysis."[6] However, DHS acts as the lead agency on cybersecurity, as well as many other areas of Internet regulation.[7]

Though privacy is highlighted in the Hathaway Report, such considerations are noticeably absent from any practical application of the Cybersecurity Act. As Senators Joseph Lieberman and Susan Collins noted in their May 1, 2008 letter to DHS Secretary Michael Chertoff, efforts to "downgrade the classification or declassify information regarding [CNCI] would … permit broader collaboration with the privacy sector and outside experts."[8] President Obama's recent focus on Transparency, Participation, and Collaboration between the public and executive agencies further justifies a renewed effort to disclose such information to the public. Releasing the documents sought in this request would provide the opportunity for meaningful public participation in the development of new security measures that may have a significant impact on civil liberties, such as privacy.[9]

---

[2] "The CNCI – officially established in January when President Bush signed National Security Presidential Directive 54 / Homeland Security Presidential Directive 23 – is a multi-agency, multi-year plan that lays out twelve steps to securing the federal government's cyber networks. DHS has been tasked to lead or play a major role in many of these tasks. This bold, much-needed approach to cyber security will lead to a fundamental shift in the way the Department approaches the security of U.S. networks." Letter from Joseph I. Lieberman, Chairman, and Susan M. Collins, Ranking Member, United States Senate Committee on Homeland Security and Governmental Affairs to Michael Chertoff, Secretary, Department of Homeland Security (May 1, 2008), *available at* http://hsgac.senate.gov/public/_files/5108LiebermanCollinslettertoChertoff.pdf.

[3] Jaikumar Vijayan, *Obama Taps Bush Aide Melissa Hathaway to Review Federal Cybersecurity Efforts*, COMPUTER WORLD: SECURITY, Feb. 9, 2009, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9127682.

[4] Jennifer Granick, *Federal Authority Over the Internet? The Cybersecurity Act of 2009*, ELECTRONIC FRONTIER FOUNDATION, Apr. 10, 2009, http://www.eff.org/deeplinks/2009/04/cybersecurity-act.

[5] *Supra* note 1.

[6] Ellen Nakashima, *Bush Order Expands Network Monitoring*, THE WASH. POST, Jan. 26, 2009, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012503261.html?wpisrc=newsletter.

[7] *See, e.g.*, Department of Homeland Security, *Cybersecurity: Make it a Habit*, Oct. 20, 2008, http://www.dhs.gov/xprevprot/programs/gc_1202746448575.shtm; Department of Homeland Security, *Internet Hoaxes*, Oct. 21, 2008, http://www.dhs.gov/xcitizens/general_1165337828628.shtm; Department of Homeland Security, *DHS Privacy Office – Privacy Workshops*, June 9, 2009, http://www.dhs.gov/xinfoshare/committees/editorial_0699.shtm.

[8] *Supra* note 2.

[9] Memoranda from Barack Obama, President of the United States, on Transparency and Open Government (January 21, 2009) *available at* http://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment/.

Although the CNCI has been the primary source of cybersecurity rules since 2008, neither it nor the authorizing Directive have been released in full.[10] Gregory Garcia (then DHS Assistant Secretary of Cybersecurity and Telecommunications) stated in February 2009 that "too much was kept secret."[11] The policy goals in the Directive, and the implementation of those goals in the CNCI, have directed virtually all cybersecurity regulation. The Senate Committee on Homeland Security and Governmental Affairs recognizes that cyber security initiatives must include actions to "…reassure [the public] that efforts to secure cyber networks will be appropriately balanced with respect for privacy and civil liberties."[12] The government cannot meaningfully make such assurances without making public the foundational documents underpinning the CNCI.

Procedural Background

On June 25, 2009, EPIC transmitted EPIC's FOIA Request to the DHS Management Directorate. *See* Appendix 1. The letter contained a request for expedited processing. *Id*. This request was re-transmitted on June 26, 2009, on the request of DHS.

On June 26, 2009, the DHS Management Directorate wrote to EPIC to acknowledge receipt of EPIC's FOIA Request and to announce a transfer of the request to the DHS Headquarters & Privacy Office. *See* Appendix 2. The DHS did not make any determination regarding EPIC's FOIA Request at that time. *See* 5 U.S.C. § 552(a)(6); *see also* Appendix 2.

On July 9, 2009, the DHS Headquarters & Privacy Office wrote to EPIC, acknowledging receipt of EPIC's FOIA Request, and notifying EPIC of its determination to refer the request to the DHS National Protection and Programs Directorate ("NPPD"), but did not make any determination regarding the substance of EPIC's FOIA Request. *See* Appendix 3; *see also* 5 U.S.C. § 552(a)(6).

EPIC Appeals the DHS's Failure to Disclose Records

EPIC hereby appeals the DHS's failure to make a timely determination regarding EPIC's FOIA Request. An agency must make a determination regarding a FOIA request within twenty working days. 5 U.S.C. § 552(a)(6); *see also Wash. Post v. Dep't of Homeland Sec.*, 459 F. Supp. 2d 61, 74 (D.D.C. 2006) (citing *Payne Enterprises v. U.S.*, 837 F.2d 486, 494 (D.C. Cir. 1998)) (stating "FOIA was created to foster public awareness, and failure to process FOIA requests in a timely fashion is 'tantamount to denial.'"). If a FOIA request is submitted for expedited processing, an agency must make a determination regarding the FOIA request within 10 calendar days. 5 U.S.C. § 552(a)(6)(E)(ii)(I).

EPIC Renews Its Request for Expedited Processing

There is particular urgency for the public to obtain information about the Initiative. The Cybersecurity Act of 2009 is presently under consideration by the Senate Committee on Commerce, Science, and Transportation (S. 773). In order for EPIC to make meaningful public

[10] *See supra* note 1.
[11] *Id.*
[12] *Supra* note 2.

comment on this or subsequent security measures, EPIC and the public must be aware of current programs. DHS has not provided information on measures adopted to safeguard the privacy of citizens' personal information in connection to the directive or CNCI. The public should be informed of DHS' ongoing role in the Initiative prior to passage of the Cybersecurity Act currently under consideration. *See* 6 C.F.R. § 5.5(d). Therefore, EPIC renews its request for expedited processing. 5 U.S.C. § 552(a)(6)(E)(ii)(I).

EPIC Renews Its Request for "News Media" Fee Status

EPIC renews its request for "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. *EPIC v. Dep't of Defense*, 241 F. Supp. 2d 5 (D.D.C. 2003).

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

Conclusion

Thank you for your prompt response to this appeal. As the FOIA expedited processing rules provide, I anticipate that you will produce responsive documents within 10 working days. If you have any questions, please feel free to contact EPIC at (202) 483-1140 or verdi@EPIC.org.

Sincerely,

_____
Amie L. Stepanovich
EPIC Clerk

_____
John Verdi
Director, EPIC Open Government Project

/enclosures

Appendix I

EPIC's June 25, 2009 FOIA Request to the DHS

Appendix 2

June 26, 2009 Letter from the DHS Management Directorate to EPIC Referring the Request to the DHS Headquarters & Privacy Office

Appendix 3

July 9, 2009 Letter from the DHS Headquarters & Privacy Office to EPIC Referring the Request to the DHS National Protection and Programs Directorate