



July 30, 2009

BY CERTIFIED MAIL

NSA/CSS FOIA Appeal Authority (DJP4)
National Security Agency
9800 Savage Road STE 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 Appeal (FOIA Case 58987)

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 National Security Agency ("NSA") by the Electronic Privacy Information Center ("EPIC").

On June 25, 2009, EPIC requested, *via facsimile*, documents regarding National Security Directive 54 (the "Directive") and the Comprehensive National Cybersecurity Initiative (the "Initiative"). Specifically, EPIC requested:

1. The text of the National Security Presidential Directive 54 otherwise referred to as 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. Any privacy policies related to either the Directive or the 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, George W. Bush issued the Directive, but it was never released to the public.¹ Under this secret Directive,² the Comprehensive National Cybersecurity Initiative

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

(CNCI) was formed to “improve how the federal government protects sensitive information from hackers and nation states trying to break into agency networks.”³ In February 2009, President Obama appointed Melissa Hathaway as the head of a 60-day review of government’s cybersecurity efforts (the Hathaway Report).⁴ In April 2009, Senator Jay Rockefeller (D-WV) introduced to Congress the Cybersecurity Act of 2009 (S. 773), still pending in the Senate Committee on Commerce, Science, and Transportation.⁵

The NSA has been involved with the development of cybersecurity policy since the Directive was issued.⁶ In fact, the Washington Post noted the NSA, along with FBI and CIA, as agencies charged with the responsibility of implementing the CNCI.⁷ The March 2009 resignation letter of the former head of the DHS National Cybersecurity Center, Rod Beckstrom, confirms that the NSA did in fact gain tremendous influence over DHS cybersecurity operations. In his letter, Mr. Beckstrom asserted that the “NSA effectively controls DHS cyber efforts through . . . technology insertions, and the proposed move of two organizations under DHS (the National Protection and Programs Directorate and the National Cybersecurity Center) to a Fort Meade NSA facility.”⁸ Therefore, NSA likely has possession and control of the documents EPIC seeks in this request.

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.”⁹ 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

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 cybersecurity 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 *Id.*

⁴ 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>.

⁵ 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>.

⁶ Jill R. Aitoro, *The Comprehensive National Cybersecurity Initiative*, NEXTGOV, June 1, 2009, http://www.nextgov.com/the_basics/tb_20090601_8569.php.

⁷ Ellen Nakashima, *Bush Order Expands Network Monitoring*, THE WASHINGTON POST, Jan. 26, 2009, *available at* <http://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012503261.html?wpisrc=newsletter>

⁸ Letter from Rod Beckstrom, Director, National Cybersecurity Center to Janet Napolitano, Secretary, Department of Homeland Security (March 5, 2009), *available at* <http://online.wsj.com/public/resources/documents/BeckstromResignation.pdf>.

⁹ *Supra* note 2.

civil liberties, such as privacy.¹⁰ The Senate Committee on Homeland Security and Governmental Affairs recognizes that cybersecurity 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.”¹¹ The government cannot meaningfully make such assurances without making public the foundational documents underpinning the CNCI.

Procedural Background

On June 29, 2009, EPIC transmitted EPIC’s FOIA Request to the NSA. *See* Appendix 1.

On July 1, 2009, the NSA wrote to EPIC, acknowledged receipt of EPIC’s FOIA Request and denied EPIC’s request for expedited processing, but did not make any substantive determination regarding EPIC’s FOIA request. *See* 5 U.S.C. § 552(a)(6); *see also* Appendix 2.

EPIC Appeals the NSA’s Failure to Disclose Records

EPIC hereby appeals the NSA’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. § 522(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.’”).

EPIC Appeals the NSA’s Denial of Its Request for Expedited Processing

EPIC appeals NSA’s refusal to grant expedited processing for its FOIA request. The 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.” 5 U.S.C. § 552(a)(6)(E)(v)(II).

EPIC is “primarily engaged in disseminating information.” *American Civil Liberties Union v. Department of Justice*, 321 F. Supp. 2d 24, 29 n.5 (D.D.C. 2004).

Moreover, 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 comment on this or subsequent security measures, EPIC and the public must be aware of current programs. Neither NSA nor the NSA has 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 NSA’s ongoing role in the Initiative prior to passage of the Cybersecurity Act currently under consideration.


¹⁰ 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/.

¹¹ *Supra* note 2.


Conclusion

Thank you for prompt response to this appeal. As the FOIA provides, I anticipate that you will produce responsive documents within 10 working days. If you have any questions, please feel free to contact me or John Verdi at (202) 483-1140 or Verdi@epic.org.

Sincerely,



Mark Perry
EPIC Clerk



John Verdi
Director, EPIC Open Government Project

/enclosures

Appendix 1

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

June 25, 2009



1718 Connecticut Ave NW

Suite 200

Washington DC 20009

USA

+1 202 483 1140 [tel]

+1 202 483 1248 [fax]

www.epic.org

June 25, 2009

VIA FACSIMILE (443.479.3612)

National Security Agency
 Attn: FOIA/PA Office (DJP4)
 9800 Savage Road, Suite 6248
 Ft. George G. Meade, MD 200755-6248

RE: Freedom of Information Act Request and Request for Expedited Processing

Dear FOIA/PA Officer:

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 National Security Presidential Directive 54 (the Directive) and related records in possession of the agency.

Background

In January 2008, George W. Bush issued the Directive, but it was never released to the public.¹ Under this secret Directive,² the Comprehensive National Cybersecurity Initiative (CNCI) was formed to "improve how the federal government protects sensitive information from hackers and nation states trying to break into agency networks."³ In February 2009, President Obama appointed Melissa Hathaway as the head of a 60-day review of government's cybersecurity efforts (the Hathaway Report).⁴ In April 2009, Senator Jay Rockefeller (D-WV)

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

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 cybersecurity 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 *Id.*

⁴ 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>.

introduced to Congress the Cybersecurity Act of 2009 (S. 773), still pending in the Senate Committee on Commerce, Science, and Transportation.⁵

The NSA has been involved with the development of cybersecurity policy since the Directive was issued.⁶ In fact, the Washington Post noted the NSA, along with FBI and CIA, as agencies charged with the responsibility of implementing the CNCI.⁷ The March 2009 resignation letter of the former head of the DHS National Cybersecurity Center, Rod Beckstrom, confirms that the NSA did in fact gain tremendous influence over DHS cybersecurity operations. In his letter, Mr. Beckstrom asserted that the “NSA effectively controls DHS cyber efforts through . . . technology insertions, and the proposed move of two organizations under DHS (the National Protection and Programs Directorate and the National Cybersecurity Center) to a Fort Meade NSA facility.”⁸ Therefore, NSA likely has possession and control of the documents EPIC seeks in this request.

Though privacy is highlighted in the Hathway 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.”⁹ 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.¹⁰ The Senate Committee on Homeland Security and Governmental Affairs recognizes that cybersecurity 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.”¹¹ The government cannot meaningfully make such assurances without making public the foundational documents underpinning the CNCI.

⁵ 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>.

⁶ Jill R. Aitoro, *The Comprehensive National Cybersecurity Initiative*, NEXTGOV, June 1, 2009, http://www.nextgov.com/the_basics/tb_20090601_8569.php.

⁷ Ellen Nakashima, *Bush Order Expands Network Monitoring*, THE WASHINGTON POST, Jan. 26, 2009, available at <http://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012503261.html?wpisrc=newsletter>

⁸ Letter from Rod Beckstrom, Director, National Cybersecurity Center to Janet Napolitano, Secretary, Department of Homeland Security (March 5, 2009), available at <http://online.wsj.com/public/resources/documents/BeckstromResignation.pdf>.

⁹ *Supra* note 2.

¹⁰ 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/.

¹¹ *Supra* note 2.

Documents Requested

Although the Initiative has been the primary source of cybersecurity rules since 2008, neither the Initiative nor the authorizing Directive has been released in full.¹² Gregory Garcia (then DHS Assistant Secretary of Cybersecurity and Telecommunications) stated in February 2009 that “too much was kept secret.”¹³ The policy goals in the Directive, and the implementation of those goals in the Initiative, have directed virtually all cybersecurity regulation. Therefore, EPIC requests copies of the following agency records:

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. Any privacy policies related to either the Directive, the 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.

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.” 5 U.S.C. § 552(a)(6)(E)(v)(II).

EPIC is “primarily engaged in disseminating information.” *American Civil Liberties Union v. Department of Justice*, 321 F. Supp. 2d 24, 29 n.5 (D.D.C. 2004).

Moreover, there is particular urgency for the public to obtain information about CNCI. The Cybersecurity Act of 2009 is presently under consideration by the Senate Committee on Commerce, Science, and Transportation. In order for meaningful public comment on this or subsequent cybersecurity measures, the public must be aware of current programs. Neither DHS nor NSA has 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 NSA’s ongoing role in CNCI.

Request for “News Media” 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).

¹² See, *supra* note 1.

¹³ *Id.*

Based on our status as a “news media” requester, we are entitled to receive the requested records with only duplication fees assessed. Further, 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.

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

Sincerely,



Mark Joseph Perry
EPIC Clerk



John Verdi
Director, EPIC Open Government Project

Appendix 2

July 1, 2009 Letter from NSA to EPIC Confirming Receipt

1. The failure to obtain the records on an expedited basis could reasonably be expected to pose an imminent threat to the life or physical safety of an individual.

2. The information is urgently needed by an individual primarily engaged in disseminating information to inform the public about actual or alleged Federal Government activity. Urgent need means that the information has a particular value that will be lost if not disseminated quickly.

A request will also be handled expeditiously, upon receipt of a certified statement by the requester, if the substantial due process rights of the requester would be impaired by the failure to process the request immediately and the information sought is not otherwise available; there is a humanitarian need which will promote the welfare and interest of mankind; or other narrowly construed exceptional circumstances exist.

Your request for expedited treatment has been denied because it does not meet the FOIA's criteria for expedited treatment. We will process your request in our normal processing queue.

The Initial Denial Authority for NSA is the Deputy Associate Director for Policy and Records, Diane M. Janosek. If you disagree with the decision regarding denial of your expedite request, you may file an appeal to the NSA/CSS Freedom of Information Act Appeal Authority. The appeal must be postmarked no later than 60 calendar days after the date of the initial denial letter. The appeal shall be in writing addressed to the NSA/CSS FOIA Appeal Authority (DJP4), National Security Agency, 9800 Savage Road STE 6248, Fort George G. Meade, MD 20755-6248. The appeal shall reference the denial and shall contain, in sufficient detail and particularity, the grounds upon which you believe expeditious processing is warranted. The NSA/CSS Appeal Authority will endeavor to respond to the appeal within 20 working days after receipt, absent any unusual circumstances.

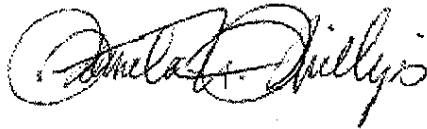
Sincerely,



PAMELA N. PHILLIPS
Chief
FOIA/PA Office

(DJP4), 9800 Savage Road STE 6248, Ft. George G. Meade, MD 20755-6248 or may be sent by facsimile to 443-479-3612. If sent by fax, it should be marked for the attention of the FOIA office. The telephone number of the FOIA office is 301-688-6527.

Sincerely,

A handwritten signature in cursive script, appearing to read "Pamela N. Phillips".

PAMELA N. PHILLIPS
Chief
FOIA/PA Office

Encls:
a/s