epic.org

1718 Connecticut Ave NW
Suite 200
Washington DC 20009
USA
+1 202 483 1140 [tel]
+1 202 483 1248 [fax]
www.epic.org

September 27, 2013

U.S. Department of Homeland Security
Washington, D.C. 20528
FOIA Officer/Public Liaison: Sandy Ford Page
Phone: 703-235-2211
Fax: 703-235-2052
E-mail: NPPD.FOIA@dhs.gov

RE: Freedom of Information Act Request

Dear Ms. Page,

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 concerning Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience ("PPD-21").

Background

On February 12, 2013, President Obama issued PPD-21.[1] PPD-21 directs various Federal agencies to create and implement a coordinated strategy for the defense of critical infrastructure.[2] To do so, it authorizes the establishment of two critical infrastructure centers to be operated by DHS, one for physical infrastructure and one for cyber infrastructure. The goal of these centers is to facilitate the exchange of information within the government and with the private sector.[3] The Directive states

> Federal departments and agencies shall implement this directive in a manner consistent with applicable law, Presidential directives, and Federal regulations, including those protecting privacy, civil rights, and civil liberties. In addition, Federal departments and agencies shall protect all information associated with carrying out

1 Presidential Policy Directive – Critical Infrastructure Security and Resilience, February 12, 2013, available at: http://epic.org/privacy/cybersecurity/PPD-21.pdf
2 *Id.* at 2.
3 *Id.* at 6.

this directive consistent with applicable legal authorities and policies."[4]

Additionally, PPD-21 facilitates the ability of the DHS to have a near real-time situational awareness of such infrastructure.[5]

Cybersecurity efforts inevitably raise privacy concerns. PPD-21 itself has raised concerns with the public over the scope to which the government will intrude upon the operations of private infrastructure owners.[6] Questions have also been raised as to how a single strategy that encompasses both physical and cyber threats can be implemented.[7]

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.[8] EPIC has previously testified to Congress on the need for privacy protections in cybersecurity efforts.[9] EPIC has also provided extensive comments to both the Department of Homeland Security and the Department of Defense on agency cybersecurity programs.[10]

PPD-21 requires deliverables at specified times. Within 120 days of release, the Secretary of Homeland Security is to develop a description of the functional relationships across the Federal government related to critical infrastructure security.[11] Within 150 days, the Secretary is to submit a report on the evaluation of the existing public-private partnership model. This evaluation includes recommendations for enhancing such partnerships.[12] Within 180 days, the Secretary shall convene a team of experts to determine the baseline

---

4 *Id.* at 7.

5 *Id.*

6 Jody Westby, Obama's Cybersecurity Action Reaches Too Far, February 13, 2013, http://www.forbes.com/sites/jodywestby/2013/02/13/obamas-cybersecurity-action-reaches-too-far/

7 Richard Stiennon, PPD 21: Extreme Risk Management Gone Bad, February 14, 2013, http://www.forbes.com/sites/richardstiennon/2013/02/14/ppd-21-extreme-risk-management-gone-bad/

8 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 (last visitedNov.14.2012).;Memorandum.Dkt.No. 9, EPIC v. NSA (No. 10-00196).

9 Cybersecurity and Data Protection in the Financial Sector: Hearing Before the Subcomm. on Financial Institution and Consumer Credit of the H. Comm. on Financial Services, 112th Congo (2011) (testimony and statement for the record of Marc Rotenberg, EPIC), available at http://financialservices.house.gov/uploadedfiles/09141/rotenberg.pdf; Cybersecurity and Data Protection in the Financial Sector: Hearing Before the S. Comm. on Banking, Housing, and Urban Affairs, 112th Congo (2011) (testimony and statement for the record of Marc Rotenberg, EPIC), available at http://epic.org/privacy/testimony/EPIC_Senate _ BankingTestimony%20 _6 _21_II.pdf.

10 Comments of EPIC, DOD-2009-0S-0183/RIN 0790-A160 (July 10,2012), available at http://epic.org/privacy/cybersecurity/EPIC-DOD-Cyber-Security-Comments.pdf; Comments of EPIC, DHS-20 I 0-0052 and DHS-2010-0053 (Dec. 15,2010), available at http://epic.org/privacy /fusion/EPIC Je _ DHS-20 I 0-0052_0053.pdf

11 Presidential Policy Directive – Critical Infrastructure Security and Resilience, February 12, 2013, available at: http://epic.org/privacy/cybersecurity/PPD-21.pdf at 8.

12 *Id.*

requirements for data sharing. This includes private sector information technology systems. Such analysis shall include the security of such systems and the protection of the privacy of such information.[13]

As the Directive was signed by the President on February 12, 2013, these reports should now be compiled and in the possession of the agency.

Documents Requested

EPIC requests copies of the following agency records:

1. The description of the functional relationships within DHS and across the Federal government related to critical infrastructure security and resilience provided to the President through the Assistant to the President for Homeland Security and Counterterrorism.

2. The evaluation of the existing public-private partnership model and the recommendations for improving the effectiveness of the partnership.

3. The analysis of the baseline data and systems requirements for the Federal Government to enable efficient information exchange provided to the President through the Assistant to the President for Homeland Security and Counterterrorism.

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 5 (D.D.C. 2003). 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," and disclosure "is not primarily in the commercial interest of the requester," any duplication fees should be waived.

The FOIA request involves information of the DHS's policies regarding cybersecurity and the protection of privacy. Responsive documents will hold a great informative value regarding activities of the government that will have a significant public impact.

Conclusion

Thank you for your consideration of this request. As 5 U.S.C. § 552(a)(6)(a) provides, I will anticipate your determination on our request within twenty (20) calendar days. For questions regarding this request, I can be contacted at 202-483-1140 x 120, or FOIA@epic.org.

13 *Id.* at 9.

Sincerely,

Julia Horwitz
EPIC Open Government Coordinator

/s/

Jack Bussell
EPIC Extern