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

March 12, 2012

Senator Patrick J. Leahy, Chairman,
Committee on the Judiciary
437 Russell Senate Office Building
Washington, D.C. 20510

Senator Chuck Grassley, Ranking Member
Committee on the Judiciary
135 Hart Senate Office Building
Washington, D.C. 20510

Dear Chairman Leahy and Ranking Member Grassley,

Thank you for holding the hearing on "the Freedom of Information Act: Safeguarding Critical Infrastructure and the Public's Right to Know." In response to your request for a written statement, we provide the following comments on the importance of the Freedom of Information Act, specifically concerning cyber security.

The Electronic Privacy Information Center ("EPIC") is a non-partisan research organization, established in 1994 to focus public attention on emerging privacy and civil liberties issues.[1] Much of EPIC's work over the years has been in support of the Freedom of Information Act and open government. EPIC pursued many Freedom of Information Act matters and litigated numerous cases.[2] EPIC has commented extensively on the proposed changes to the Department of Justice Freedom of Information Act regulations.[3] EPIC publishes a leading Freedom of Information Act litigation manual.[4] And we help train the next generation of Freedom of Information Act advocates and practitioners.[5]

Next week, we will be arguing before the D.C. Circuit in support of a narrow interpretation of the so-called "Glomar" doctrine.[6] We believe that the National Security Agency has improperly withheld from the American public information that should properly be released under the Freedom of Information Act. As the Congress is now considering cybersecurity legislation, we are grateful that you have taken the opportunity of Sunshine week to draw attention to the need for open and accountable government.

---

[1] EPIC, About EPIC, http://www.epic.org/epic/about.html (last visited Mar. 12, 2012).
[2] EPIC, EPIC FOIA Cases, http://epic.org/foia/ (last visited Mar. 12, 2012).
[3] Comments of the Electronic Privacy Information Center to the Department of Justice on "Revision of Department of Justice Freedom of Information Act Regulations" (Oct. 18, 2011), *available at* http://epic.org/foia/EPIC-DOJ-FOIA-Comments-FINAL.pdf.
[4] Harry A. Hammitt, Ginger McCall, Marc Rotenberg, *et. al, Litigation Under the Federal Open Government Laws* 2010 (EPIC 2010).
[5] EPIC, Jobs / IPIOP, http://epic.org/epic/jobs.html (last visited Mar. 12, 2012).
[6] *EPIC v. NSA*, Civ. Action No. 11-5233 (D.C. Cir. Sept. 9, 2011).

I. The Freedom of Information Act is Vital to Ensuring an Accountable and Transparent Government

Since the enactment of the Freedom of Information Act, Presidents have acknowledged the importance of open government to democracy. In signing the Freedom of Information Act in 1966, President Johnson acknowledged, "this legislation springs from one of our most essential principles: a democracy works best when the people have all the information that the security of the nation will permit."[7] When President Gerald R. Ford signed the Government in the Sunshine Act of 1976, amending the Freedom of Information Act, he asserted, "the decision-making business of regulatory agencies can and should be open to the public."[8] President Ford also showed particular concern over the language of Exemption Three, an issue now before this Committee, declaring that it "may well be more inclusive than necessary."[9] And President Clinton recognized that "the Freedom of Information Act was the first law to establish an effective legal right of access to government information, underscoring the crucial need in a democracy for open access to government information by citizens."[10]

When President Obama took office in 2008, he committed his administration to the importance of transparency in government. On his first day in office, President Obama issued a memorandum about the importance of the Freedom of Information Act. He explained, "At that heart of that commitment [to transparency] is the idea that accountability is in the interest of the Government and the citizenry alike."[11]

To further these goals, President Obama called for new guidelines for implementing Freedom of Information Act.[12] The guidelines issued by Attorney General Holder establish a "presumption of openness" governing federal records.[13] The Attorney General strongly encouraged agencies to make discretionary disclosures of information to the fullest extent possible. The memorandum directs that each agency is fully accountable for its administration of the Freedom of Information Act and should be mindful of their obligation to work "in a spirit of cooperation."[14]

---

[7] Signing Statement by President Lyndon Johnson on the Passage of S. 1160 the Freedom of Information Act (July 4, 1966), *available at* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB194/Document%2031.pdf.
[8] Signing Statement by President Gerald Ford on the Passage of S. 5 the Sunshine Act (Sept. 13, 1976), *available at* http://www.presidency.ucsb.edu/ws/index.php?pid=6325#axzz1oqLMGQp2.
[9] *Id.*
[10] Signing Statement by President William Clinton on the Passage of H.R. 3802 the Electronic Freedom of Information Act Amendments of 1996 (Oct. 2, 1996), *available at* http://www.gwu.edu/~nsarchiv/nsa/foia/presidentstmt.pdf.
[11] Memorandum from President Barack Obama to the Heads of Executive Departments and Agencies on Transparency and Open Government (Jan. 21, 2008), *available at* http://www.whitehouse.gov/the_press_office/Transparency_and_Open_Government/.
[12] *Id*.
[13] Memorandum from Attorney General Eric Holder to Heads of Executive Departments and Agencies on Transparency and Open Government (Mar. 19, 2009), *available at* http://www.usdoj.gov/ag/foia-memo-march2009.pdf.
[14] *Id.*

The Freedom of Information Act has been responsible for uncovering numerous cases of government fraud and abuse since its inception. Through proper and efficient use of the Freedom of Information Act, EPIC has brought to the public's attention many such matters:

- **Intelligence Oversight Board Records Revealed that the FBI was not in Compliance with Attorney General Guidelines.** EPIC obtained internal reports of intelligence law violations that the Federal Bureau of Investigation sent to the Intelligence Oversight Board. The documents detail intelligence practices that do not comply with Attorney General Guidelines.[15]

- **United States State Department Discloses Report on Obama Passport Breach.** EPIC's Freedom of Information Act lawsuit against the State Department produced a report detailing security breaches of passport data for several presidential candidates. Previously secret sections state, "the Department was ineffective at detecting possible incidents of unauthorized access," and criticized the agency's failure to "provide adequate control or oversight."[16]

- **General Services Administration Records Revealed that Feds Exempted Social Media Companies from Privacy Requirements.** In response to EPIC's Freedom of Information Act request, the General Services Administration released several contracts between the federal government and web 2.0 companies. Some of the agreements permit companies to track users of government websites for advertising purposes.[17]

- **Federal Bureau of Investigation Records Reveal Restriction of Virginia Transparency and Privacy Laws for Fusion Center.** A document obtained by EPIC from the Virginia Department of State Police reveals that the State Police entered into a secret agreement with the Federal Bureau of Investigation to impose federal restrictions on rights granted by Virginia open government and privacy laws.[18]

These revelations, and many more, were only possible through the meaningful application of the Freedom of Information Act. We will discuss the significant cybersecurity Freedom of Information Act matters EPIC has pursued in more detail below.

---

[15] *Intelligence Oversight Board: FOIA Documents Detailing Legal Violations*, ELEC. PRIVACY INFO. CTR., http://epic.org/foia/iob/default.html (last visited Mar. 12, 2012).
[16] *EPIC Forces Disclosure of Report on Obama Passport Breach*, ELEC. PRIVACY INFO. CTR., http://epic.org/open_gov/foiagallery2011.html#passport (last visited Mar. 12, 2012).
[17] *Feds Exempt Social Media Companies from Privacy Requirements*, ELEC. PRIVACY INFO. CTR., http://epic.org/open_gov/foiagallery2010.html#social (last visited Mar. 12, 2012).
[18] *EPIC v. Virginia Department of State Police: Fusion Center Secrecy Bill*, ELEC. PRIVACY INFO. CTR., http://epic.org/privacy/virginia_fusion/ (last visited Mar. 12, 2012).

II. There is a Considerable Public Interest in the Transparency of Government Cybersecurity Operations

The efforts by the government to protect our nation's critical infrastructure affect every citizen in the United States, whether or not they actually use the Internet. Information that provides details on cybersecurity threats and the failure of important information systems and databases is invaluable to every member of the U.S. population, a fact recognized by both Democrats and Republicans in the introduction and support of federal data breach notification bills.[19] People have a right to know about government decisions that impact their safety and their security.

On May 29, 2009, President Barack Obama announced the Administration's plan to address the growing issue of digital information insecurity.[20] Discussing the plan in 2010, Cybersecurity Coordinator Howard Schmidt emphasized the importance of transparency:

> Transparency is particularly vital in areas, such as the [Comprehensive National Cybersecurity Initiative], where there have been legitimate questions about sensitive topics like the role of the intelligence community in cybersecurity. Transparency provides the American people with the ability to partner with government and participate meaningfully in the discussion about how we can use the extraordinary resources and expertise of the intelligence community with proper oversight for the protection of privacy and civil liberties.[21]

Transparency and accountability in cybersecurity operations will promote security and encourage companies to implement meaningful data practices that reduce the risk of cybersecurity incidents. Companies must understand that at risk are not only their own records, but also information concerning their clients, customers, and users. For this reason, any proposal to reduce the information available to the public currently available under the Freedom of Information Act concerning cybersecurity risks should be viewed with skepticism.

III. Congress Recently Adopted a Narrow Exemption Three Statute for Critical Infrastructure

Congress has already passed an adequate Exemption Three statute to protect sensitive critical infrastructure information from disclosure under the Freedom of

---

[19] *See*, *e.g.*, Data Accountability and Trust Act (DATA), H.R. 1707, 112th Cong. (2011) (introduced by Rep. Rush (D-IL)); Secure and Fortify Electronic Data Act (SAFE Data Act) H.R. 2577, 112th Cong., (2011) (introduced by Rep. Bono Mack (R-CA)).

[20] WHITE HOUSE, CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[21] Howard A. Schmidt, *Transparent Cybersecurity*, NAT'L SEC. COUNCIL (Mar. 2, 2010), http://www.whitehouse.gov/blog/2010/03/02/transparent-cybersecurity.

Information Act.[22] Precisely, the exemption in the 2012 National Defense Authorization Act allows agencies to withhold "Department of Defense critical infrastructure" only:

> upon a written determination that the disclosure of such information would reveal vulnerabilities in such infrastructure that, if exploited would reveal vulnerabilities in such infrastructure that, if exploited, could result in the disruption, degradation, or destruction of Department of Defense operations, property, or facilities.[23]

While we would have preferred no such exemption, this provision is narrowly constructed to achieve the desired result. The legislation recognizes both the interests of ensuring the protection of "truly sensitive government information" and "allowing public access to important information about potential health and safety threats."[24]

IV. Pending Cybersecurity FOIA Proposals Would Limit Government Transparency and Accountability

The current cybersecurity legislative proposals contain Freedom of Information Act exemptions that are over-broad and will limit both accountability and transparency in United States cybersecurity operations. Notably, while most of the cybersecurity bills currently under consideration attempt to block any public access to cyber threat information, the provisions encourage the increased transfer of information to and between the private sector and the federal and state governments without any accountability for the negligent or willful misuse of that information.[25]

A. The Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology (SECURE IT) Act of 2012

The SECURE IT Act seeks to amend the Freedom of Information Act in an unprecedented manner by adding a tenth exemption for "information shared with or

---

[22] The Homeland Security Act of 2002 also contains an Exemption Three provision for voluntarily shared critical infrastructure information. Specifically, the Act protects "critical infrastructure information (including the identity of the submitting person or entity) that is voluntarily submitted to a covered Federal agency for use by that agency regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency, study, recovery, reconstitution, or other informational purpose." 6 U.S.C. § 133(a)(1) (2011).

[23] National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81.

[24] Press Release, Sen. Patrick Leahy, Balancing Security And Open Government In The Cyber Age (Mar. 6, 2012), *available at* http://www.leahy.senate.gov/press/press_releases/release/?id=4add311a-6a53-4d37-aff6-09172c984c9d.

[25] *See* Cybersecurity Act of 2012, S. 2105, 112th Cong. § 704(f) (2012), *available at* http://www.govtrack.us/congress/billtext.xpd?bill=s11262105 [hereinafter *Cybersecurity Act of 2012*] (creating liability only for knowing *and* willful violations of the Act); Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology (SECURE IT) Act of 2012, S. 2151, 112th Cong. § 102(g) (2012) [hereinafter *SECURE IT Act*] (no liability for "use, receipt, or disclosure of any cyber threat information.").

provided to a cybersecurity center."[26] The SECURE IT Act also contains a proposed Exemption Three provision that would specifically exempt all "cyber threat information" shared with the government from disclosure.[27] "Cyber threat information" is defined broadly, and could include a large amount of information unrelated to cybersecurity.[28] And without any precedent, this new provision would be mandatory, prohibiting agencies from disclosing information even would it could be made routinely available. Such language could easily produce absurd results if, for example, an agency prepares a document that it is intended to be publically available and to assist the public respond to cyber threats. According to this proposed amendment, the agency would be prohibited from providing to the public under the Freedom of Information Act a public document that would assist in countering cyber threats. It is hard to imagine a more ill conceived policy.

In a letter to Senator McCain, the bill's author, civil libertarian groups explain the damaging effect the SECURE IT Act would have on government transparency:

> As drafted, S.2151 cuts off all public access to information in cybersecurity centers before the public has a chance to understand the types of information that are covered by the bill. Much of the sensitive information likely to be shared in the cybersecurity centers is already protected from disclosure under the [Freedom of Information Act]; other information that may be shared could be critical for the public to ensure its safety. Unnecessarily wide-ranging exemptions of this type have the potential to harm public safety and national defense more than enhance those interests; the public is unable to assess whether the government is adequately combating cybersecurity threats and, therefore, unable to assess whether or how to participate in that process.

EPIC fully supports the views expressed by these organizations and strongly recommends against the adoption of Freedom of Information Act amendments that are so clearly counter-productive as the public faces growing concerns about cybersecurity.

B. The Proposed Cybersecurity Act of 2012

The proposed Cybersecurity Act of 2012 contains an Exemption Three provision in order to exempt from disclosure "any cybersecurity threat indicator disclosed by a non-Federal entity to a cybersecurity exchange."[29] The definition of "cybersecurity threat indicator" largely resembles that of "cyber threat information"

---

[26] SECURE IT Act of 2012, *supra* n. 25 at § 105.
[27] *Id.* at § 102(c)(4).
[28] *Id*. at § 101 (5); *see also* Elinor Mills, *Civil Liberties Groups: Proposed Cybersecurity Bill Is Too Broad*, CNET NEWS (Feb. 23, 2012), *available at* http://news.cnet.com/8301-27080_3-57384137-245/civil-liberties-groups-proposed-cybersecurity-bill-is-too-broad/ (as described below, the definition of "cybersecurity threat information" largely mirrors the definition of "cyber threat indicator" found in the Cybersecurity Act of 2012.
[29] Cybersecurity Act of 2012, *supra* n. 25 at § 704(d).

in the SECURE IT Act.[30] In order to prevent abuse of discretion, the implementation of both definitions would have to be subject to public scrutiny and oversight, the exact mechanisms the Freedom of Information Act exemptions would prevent.

The original purpose of Exemption Three was to provide for the continued use of non-disclosure or confidentiality provisions already included in other statutes. The Sunshine in Government Initiative estimates that over 240 Exemption Three statutes are currently active in federal law, and that each year federal department and agencies citing to "roughly 140 statutes to deny thousands of requests for information."[31]

V. EPIC, NSA, and the Freedom of Information Act: The Agency Remains a "Black hole" for Public Information about Cybersecurity

Over the years, EPIC has pursued numerous Freedom of Information Act matters with the NSA. We have done this because the NSA has played an increasingly significant role in domestic communications security. While we respect the technical expertise of the Agency, we also believe that it is vitally important that the NSA, like all federal agencies, remain accountable to the American public, particularly now that the agency has directed its extraordinary listening and processing capabilities to the private communications of the American public.

Between January 2009 and the hearing today, EPIC has pursued seven Freedom of Information Act requests with the NSA, concerning the NSA's cybersecurity operations. In six of those cases, the NSA has never disclosed documents responsive to EPIC's request. The NSA continually ignored the Freedom of Information Act's statutory deadlines or improperly refused to comply with required procedures. The NSA's actions in response to legitimate requests under the Freedom of Information Act have been evasive and egregious.

Of greatest significance, the agency has failed to provide documents to the public that are subject to disclosure under the Freedom of Information Act.

A. EPIC's FOIA Request for National Security Presidential Directive 54

The NSA has refused to release to the public even the Agency's legal basis, established by former President George W. Bush, which grants the authority for the NSA to conduct cybersecurity operations within the United States.

On June 25, 2009, EPIC submitted a Freedom of Information Act request to the NSA asking National Security Presidential Directive 54 (NSPD 54). NSPD 54 grants the NSA

---

[30] *Id.* at § 708(6). For concerns on this definition, *see Civil Liberties Groups: Proposed Cybersecurity Bill is Too Broad*, *supra* note 28.

[31] *See* National Academy of Public Administration: Open Government Dialogue, *The Administration Should Curb New Exemptions From FOIA*, http://opengov.ideascale.com/a/dtd/The-administration-should-curb-new-exemptions-from-FOIA/3194-4049 (last visited Mar. 9, 2012).

broad authority over the security of American computer networks. The Directive created the Comprehensive National Cybersecurity Initiative (CNCI), a "multi-agency, multi-year plan that lays out twelve steps to securing the federal government's cyber networks." Neither NSPD 54 nor the CNCI has ever been released in whole.

Senators had previously noted that efforts to "downgrade the classification or declassify information regarding [CNCI] would…permit broader collaboration with the privacy sector and outside experts."[32] Only after EPIC filed a lawsuit against the NSA for their mishandling of EPIC's Request did the White House release a partially de-classified version of the CNCI. Among other things, the released version of the CNCI set forth EINSTEIN 3, the government's effort to conduct "real-time packet inspection" of all government Internet traffic.[33]

Although EPIC has still not received NSPD-54, we believe it is vitally important that the NSA provide to the public, at a minimum, the legal basis of its authority to conduct cybersecurity within the United States. As we have repeatedly stressed in our filings, we simply cannot accept a doctrine of "secret law" in the United States for such a critical government function.

B. EPIC's FOIA Request for the Testimony of Lieutenant General Keith Alexander

On April 16, 2010, EPIC requested from the NSA the "classified supplement" of Lieutenant General Keith Alexander, containing his answers to questions posed by the Senate Armed Service Committee in a hearing on his nomination to the position of NSA Director and Chief of the Central Security Service and Commander of the United States Cyber Command (CYBERCOM).

Much of Lieutenant General Alexander's public testimony raised questions about the growing influence of the military in civilian cybersecurity efforts, including an emphasis on the need to "be prepared to provide military options…if our national security is threatened."[34] When asked about the deployment of classified methods of monitoring electronic communications, most of the Lieutenant General's response was classified. Despite the notable public interest in the practice of monitoring Internet traffic, the NSA has again refused to make this information available to the public.

C. EPIC's FOIA Requests Cybersecurity Risk Assessments

---

[32] 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.

[33] WHITE HOUSE, THE COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE, *available at* http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

[34] Advance Questions for Lieutenant General Keith Alexander, USA Nominee for Commander, United States Cyber Command (Unclassified), *available at* http://senate.gov/~armed_services/statemnt/2010/04%20April/Alexander%2004-15-10.pdf.

The NSA has also locked relationships and agreements with private industry away. Under the National Strategy to Secure Cyberspace, the NSA was given the authority to provide technical assistance to owners of national security systems and conduct vulnerability assessments of those systems and disseminate information on threats to and vulnerabilities of national security systems.[35] Reports have confirmed the NSA's role in providing risk assessments to private industry.[36]

EPIC requested from the NSA all policies and procedures used to conduct vulnerability assessments or penetration tests on private networks. [37] Despite the White House's acknowledgement of the value of public participation in the cybersecurity process, again no documents were disclosed.

D. EPIC's FOIA Request for NSA Internet Wiretapping

In 2010, the NSA was developing new regulations, in cooperation with the Federal Bureau of Investigation and the Department of Justice, in order to require "all services that enable communications – including encrypted e-mail transmitters like BlackBerry, social networking Web sites like Facebook, and software that allows direct 'peer to peer' messaging like Skype – to be technically capable of complying if served with a wiretap order."[38]

EPIC requested the text of this proposal in order to educate the public on the issue in light of its upcoming submission to Congress and its imminent far-reaching impact on all Internet users. Despite a request for expedited treatment, the NSA has not yet disclosed any documents in response to EPIC's request.

E. EPIC v. NSA: The NSA-Google Cybersecurity Relationship

On January 12, 2010, Google reported that the company had suffered a "highly sophisticated and coordinated" cyber attack originating from China. The attackers planted malicious code in Google's corporate networks, and resulted in the theft of Google's intellectual property, and at least the attempted access of the Gmail accounts of Chinese human rights activists. The following day, Google changed a key setting, causing all subsequent traffic to and from its electronic mail servers to be encrypted by default. On

---

[35] Dept. of Homeland Security, The National Strategy to Secure Cyberspace, *available at* http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf (2003).
[36] Ellen Nakashima, *Google to Enlist NSA to Help It Ward off Cyberattacks*, Wash. Post., Feb. 4, 2010, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03/AR1010020304057.html.
[37] Executive Office of the President, Cyberspace Policy Review (2009) at C-7 n. 28, *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf ("People cannot value security without first understanding how much is at risk.").
[38] Charlie Savage, *U.S. Tries to Make it Easier to Wiretap the Internet*, New York Times, Sept. 27, 2010, http://www.nytimes.com/2010/09/27/us/27wiretap.html?_r=1&ref=technology; Ellen Nakashima, *U.S. Seeks Ways to Wiretap the Internet*, Washington Post, Sept. 28, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/09/27/AR2010092706637.html.

February 4, 2010, the Washington Post reported that Google had contacted the National Security Agency ("NSA") regarding the firm's security practices immediately following the attack. In addition, the Wall Street Journal stated that the NSA's general counsel had drafted a "cooperative research and development agreement" within 24 hours of Google's announcement of the attack, which authorized the Agency to "examine some of the data related to the intrusion into Google's systems."

EPIC submitted a Freedom of Information request to the NSA requesting documents that pertained to the relationship between the NSA and Google. The NSA responded to EPIC's Freedom of Information Act request by issuing a Glomar response – refusing to confirm or deny that records existed. The NSA broadly defined their authority to operate secretly to an unprecedented degree, claiming that it was not even necessary to search for documents before making a substantive decision on what those documents may contain.

The NSA's claims would allow the agency to exercise unfettered discretion to dismiss any Freedom of Information request brought before it. For this reason, EPIC will be arguing before the DC Circuit next week in support of the public's right to know about the cyber security decisions that may determine, for example, whether a federal agency believes individual users should routinely encrypt their email.

F. ThinThread and Trailblazer

Even when the NSA publicly announces a surveillance program, the Agency's procedures under the Freedom of Information Act have shielded key documents from the public. As far back as 2000, the NSA implemented surveillance programs code-named ThinThread and Trailblazer in order to collect large quantities of data from various sources – financial transactions, travel records, web searches, and GPS equipment.[39] The pilot program, ThinThread, was abandoned in 2000 due to concerns of legality, and replaced by Trailblazer.[40] After having received a request from EPIC for contracts, agreements, and technical specifications regarding how information was gathered and used under the programs, the NSA failed to produce responsive.

The NSA's failure to provide information to the public about these programs may have also undercut efforts to promote cyber security in the United States.

G. EPIC FOIA Request for the NSA's "Perfect Citizen" Program

In 2010, the NSA recently completed a contract to develop "a set of sensors deployed in computer networks for critical infrastructure that would be triggered by

[39] Siobhan Gorman, *NSA Killed System That Sifted Phone Data Legally*, The Baltimore Sun, May 18, 2006, *available at* http://www.baltimoresun.com/news/nationworld/bal-nsa517,0,5970724.story?coll=bal-home-headlines.
[40] *Id*.

unusual activity suggesting an impending cyber attack."[41] The company that the NSA was contracting with, Raytheon, described the program as "Big Brother."[42] The program was to be funded as part of the CNCI, the White House's cybersecurity plan that the NSA refused to release in full to the public under a separate EPIC FOIA request.[43] EPIC has requested, but not received, the contracts under which the program was formed and any analyses or legal memoranda related to it.

The NSA's practices in response to requests for information under the Freedom of Information Act paint a picture of an Agency shrouded in secrecy that refuses to disclose even documents that are demonstrably vital to facilitating public involvement in the cybersecurity. The broad assertion of Section 6 of the NSA Act, the agency's Exemption Three statute for Freedom of Information Act purposes, is a reminder of what government agency's do with secrecy: they keep the public in the dark even as their own programs flounder and fail.

EPIC's experience over the last several years trying to obtain relevant information from the NSA concerning cybersecurity activities that directly impact the American public is a clear warning about the dangers of government secrecy. We strongly urge the Congress to maintain its vigorous defense of openness and agency accountability. While it may be tempting to establish new forms of government secrecy to respond to new threats, those changes are more likely to cause new problems than to offer workable solutions.

Thank you for your consideration of our views. We will provide additional information as it becomes available.

Sincerely,

/s/
Marc Rotenberg
EPIC Executive Director

/s/
Ginger McCall
Director, EPIC Open Government Project

/s/
Amie Stepanovich
EPIC National Security Counsel

---

[41] Siobhan Gorman, *U.S. Program to Detect Cyber Attacks on Infrastructure*, Wall St. J., July 8, 2010, *available at* http://online.wsj.com/article/SB10001424052748704545004575352983850463.html.
[42] *Id*.
[43] *See supra* pp. 7-8.