

Office of the Director of National Intelligence  
Washington, DC 20511

FEB 04 2015

Ms. Rita Cant  
American Civil Liberties Union Foundation  
125 Broad Street, 18th Floor  
New York, NY 10004

Re: ODNI FOIA request DF-2014-00191

Dear Ms. Cant:

This responds to your facsimile to the Office of the Director of National Intelligence (ODNI), dated 29 April 2014 (Enclosure), in which you requested, under the Freedom of Information Act (FOIA), **“disclosure of guidance or directives that set forth the government’s policies regarding the purchase, discovery disclosure and exploitation of “zero-day” vulnerabilities—security flaws in computer software that are unknown to the software’s programmers and users.”**

Your request was processed in accordance with the FOIA, 5 U.S.C. § 552, as amended. A thorough search of our records and databases located documents responsive to your request. One document has been referred to another agency for review and direct response to you.

The remaining documents were reviewed and found to contain information that is currently and properly classified under Executive Order 13526, Section 1.4(c), and is therefore withheld pursuant to FOIA exemption (b)(1). Information was also withheld pursuant to the following FOIA exemptions:

- (b)(3), which applies to information exempt from disclosure by statute, specifically the National Security Act of 1947, as amended, 50 U.S.C. § 3024(m)(1), which protects, among other things, the names and identifying information of ODNI personnel; and
- (b)(6), which applies to records which, if released, would constitute a clearly unwarranted invasion of the personal privacy of individuals.

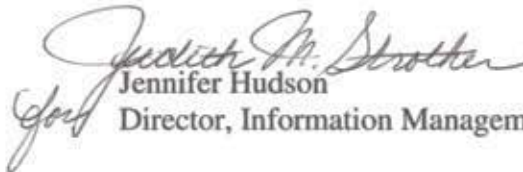
Finally, as the documents are entirely deliberative, they have been withheld in full pursuant to FOIA exemption (b)(5), which protects privileged interagency or intraagency information.

You may appeal our determination within 45 days of the date of this letter by sending a written appeal letter, citing the basis of the appeal to the address below:

Office of the Director of National Intelligence  
Information Management Office  
Washington D.C. 20511

If you have any questions, please email our Requester Service Center at [DNI-FOIA@dni.gov](mailto:DNI-FOIA@dni.gov) or call us at (703) 874-8500.

Sincerely,

  
Jennifer Hudson  
Director, Information Management Division

Enclosure

# ENCLOSURE

1



APR 30 2014

DF.2014-00191

**National Headquarters**  
Legal Department  
125 Broad Street • New York, NY 10004

FAX: (212) 549-2654

### FAX TRANSMITTAL SHEET

**TO:** Office of the Director of National Intelligence  
Information Management Division  
Attn: Jennifer L. Hudson  
Washington, D.C. 20511  
**FAX NUMBER:** (703) 874-8910  
**FROM:** Rita Cant, American Civil Liberties Union  
**DATE:** April 29, 2014

**Total number of pages (including this cover page): 11**

---

In this fax, please find a Freedom Of Information Act request.

This transmission is intended for the sole use of the individual and entity to whom it is addressed, and may contain information that is privileged, confidential and exempt from disclosure under applicable law. You are hereby notified that any dissemination, distribution or reproduction of this transmission by someone other than the addressee or its designated agent is strictly prohibited.



April 29, 2014

**VIA FACSIMILE**

Office of the Director of National Intelligence  
Information Management Division  
Attn: Jennifer L. Hudson  
Washington, D.C. 20511

Fax: (703) 874-8910

National Security Agency / Central Security Service  
NSP5 / FOIA Requester Services  
9800 Savage Road, Suite 6248  
Fort George G. Meade, MD 20755-6248

Fax: (301) 688-4762

U.S. Strategic Command  
J006 (FOIA)  
901 Sac Boulevard Suite 2E27  
Offutt Air Force Base, NE 68113

Fax: (402) 294-7535

Department of Justice  
FOIA/PA Mail Referral Unit  
Room 115, LOC Building  
Washington, D.C. 20530-0001

Fax: (301) 341-0772

Office of Legal Counsel  
Attn: Elizabeth Farris  
Room 5515, 950 Pennsylvania Avenue, N.W.  
Washington, D.C. 20530-0001

Fax: (202) 514-0539

Federal Bureau of Investigation  
FOI/PA Request, Record/Information Dissemination Section  
170 Marcel Drive  
Winchester, VA 22602-4843

Fax: (540) 868-4391

Department of Homeland Security  
The Privacy Office  
245 Murray Lane S.W., Stop 0655  
Washington, D.C. 20528-0655

Fax: (703) 235-0443

Immigration and Customs Enforcement  
Freedom of Information Act Office  
500 12th Street S.W., Stop 5009  
Washington, D.C. 20536-5009

Fax: (202) 732-4265

AMERICAN CIVIL LIBERTIES  
UNION FOUNDATION  
NATIONAL OFFICE  
110 BROAD STREET 10TH FL  
NEW YORK NY 10004-2400  
TEL: 212 542 2500  
WWW.ACLU.ORG



**Re: REQUEST UNDER THE FREEDOM OF INFORMATION ACT**

To Whom It May Concern:

Under the Freedom of Information Act, the American Civil Liberties Union and the American Civil Liberties Union Foundation (collectively, "ACLU") request disclosure of guidance or directives that set forth the government's policies regarding the purchase, discovery, disclosure, and exploitation of "zero-day" vulnerabilities—security flaws in computer software that are unknown to the software's programmers and users. On April 11, the White House formally acknowledged the existence of a process for agencies to decide when to disclose security vulnerabilities and when to hold them in secret for government exploitation.<sup>1</sup> This process was the subject of a recent White House review, the conclusions of which are reportedly documented in a presidential directive.<sup>2</sup>

AMERICAN CIVIL LIBERTIES  
UNION FOUNDATION

When vulnerabilities remain concealed from the programmers responsible for the software, they may be exploited by governments for military, intelligence, or law-enforcement purposes. They also may be exploited by criminals engaging in cyber attacks. According to senior government officials, cyber attacks are one of the gravest threats facing the country today.<sup>3</sup> Release of the requested documents will help Americans understand if the government's zero-day policy works to protect them, or works against them by increasing their vulnerability to cyber attacks.

<sup>1</sup> See Press Release, Office of Dir. Nat'l Intel. ("ODNI"), Statement on Bloomberg News Story That NSA Knew About the "Heartbleed Bug" Flaw and Regularly Used It to Gather Critical Intelligence (Apr. 11, 2014), <http://iconthecrccord.tumblr.com/post/82416436703/statement-on-bloomberg-news-story-that-nsa-knew>.

<sup>2</sup> See Michael Riley, *Trove of Software Flaws Used by U.S. Spies at Risk*, Bloomberg, Apr. 14, 2014, 12:00 AM, <http://www.bloomberg.com/news/2014-04-14/president-s-security-flaw-guidance-seen-hard-to-implement.html>.

<sup>3</sup> See Jim Garamone, *Clapper Places Cyber at Top of Transnational Threat List*, Armed Forces Press Service, Mar. 12, 2013, <http://www.defense.gov/news/newsarticle.aspx?id=119500>. See also Greg Miller, *FBI Director Warns of Cyberattacks; Other Security Chiefs Say Terrorism Threat Has Altered*, Wash. Post, Nov. 14, 2013, [http://www.washingtonpost.com/world/national-security/fbi-director-warns-of-cyberattacks-other-security-chiefs-say-terrorism-threat-has-altered/2013/11/14/24f1b27a-4d53-11e3-9890-a1e0997fb0c0\\_story.html](http://www.washingtonpost.com/world/national-security/fbi-director-warns-of-cyberattacks-other-security-chiefs-say-terrorism-threat-has-altered/2013/11/14/24f1b27a-4d53-11e3-9890-a1e0997fb0c0_story.html) ("FBI Director James B. Comey testified . . . that the risk of cyberattacks is likely to exceed the danger posed by al-Qaeda and other terrorist networks as the top national security threat to the United States and will become the dominant focus of law enforcement and intelligence services.").

## I. Background

Zero-day vulnerabilities are security flaws in software that have not been reported to the company, organization, or developer responsible for maintaining the software.<sup>4</sup> By definition, there is no readily available defense to unknown security flaws. Accordingly, zero-day vulnerabilities can be used to gain unauthorized access to otherwise secure systems, exposing sensitive information such as usernames and passwords, the contents of email inboxes, and medical and bank account records, and as well as commercial trade secrets and other proprietary information.<sup>5</sup>

For these reasons, zero-day vulnerabilities are highly sought after by cyber criminals and governments alike.<sup>6</sup> When military, intelligence, or law enforcement agencies buy and stockpile zero-day vulnerabilities, however, they do so in lieu of reporting the vulnerabilities to programmers responsible for the software. The failure to report in turn prevents programmers from fixing—"patching"—their software to protect their customers and other users from cyber attacks.

This tradeoff means that the policy choice to buy and stockpile zero-day vulnerabilities rather than report software vulnerabilities, is, in effect, a choice to leave the internet and all of its users less secure. As the President's Review Committee on Intelligence and Communications Technologies observed: "A vulnerability that can be exploited on the battlefield can also be exploited elsewhere."<sup>7</sup>

The Review Committee recently urged the White House to re-evaluate its policies regarding zero-days, finding "in almost all instances" that "it is in the national interest to eliminate software vulnerabilities rather than to use them for US intelligence collection."<sup>8</sup> According to the Review Committee, responsibly disclosing security vulnerabilities to the appropriate software programmers would "strengthen[ ] the security of US Government, critical infrastructure, and other computer systems."<sup>9</sup> In its final report, the Review Committee recommended that "US policy should generally move to

<sup>4</sup> See Layla Bilge & Tudor Dumitras, *Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World*, Symantec Research Labs, Oct. 16, 2012, [http://users.ece.cmu.edu/~tdumitras/public\\_documents/bilge12\\_zero\\_day.pdf](http://users.ece.cmu.edu/~tdumitras/public_documents/bilge12_zero_day.pdf).

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

<sup>6</sup> See, e.g., Joseph Menn, *U.S. Cyberwar Strategy Stokes Fear of Blowback*, Reuters, May 10, 2013, <http://www.reuters.com/article/2013/05/10/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510>; Reva Rivman, *The RSA Hack: How They Did It*, N.Y. Times Bits Blog, Apr. 2, 2011, [http://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/?\\_php=true&\\_type=blogs&\\_r=0](http://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/?_php=true&_type=blogs&_r=0).

<sup>7</sup> Review Grp. on Intelligence and Comm'n Techs., *Liberty and Security in a Changing World* 187 (2013), available at [http://www.whitehouse.gov/sites/default/files/docs/2013-12-12\\_rg\\_final\\_report.pdf](http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf).

<sup>8</sup> *Id.* at 220.

<sup>9</sup> *Id.*



ensure that Zero Days are quickly blocked, so that the underlying vulnerabilities are patched on US Government and other networks.”<sup>10</sup>

## II. ‘Heartbleed’ and the President’s Zero-Day Directive

A vulnerability known as “Heartbleed” has focused national attention on the serious risks associated with security flaws in commonly used software. On April 7, 2014, security researchers reported a programming error in OpenSSL, an encryption software library relied upon by millions to protect data and communications as they are transmitted over the internet. The vulnerability causes affected servers to “leak” potentially sensitive information when communicating with an intruder attempting to connect to the servers.<sup>11</sup> Because of OpenSSL’s ubiquity, as many as two-thirds of the world’s websites—including the websites of online businesses, social networks, major banks, and the U.S. government—may have been rendered vulnerable to “Heartbleed” attacks.<sup>12</sup>

AMERICAN CIVIL LIBERTIES  
UNION FOUNDATION

Media reports that followed suggested the government had known of and concealed the existence of “Heartbleed” for its own intelligence exploits.<sup>13</sup> The White House denied all prior knowledge of the vulnerability.<sup>14</sup> In an April 11 statement, the government claimed that a discovery such as “Heartbleed” would have been shared with the software’s developers pursuant to internal disclosure policies.<sup>15</sup> This statement appears to be the first official acknowledgement of an official policy or guidance on the use of zero-days.<sup>16</sup>

<sup>10</sup> *Id.* at 37 (Recommendation 30).

<sup>11</sup> *Economist*, *Digital Heart Attack*, Apr. 12, 2014, <http://www.economist.com/news/business/21600691-flaw-popular-internet-security-software-could-have-serious-consequences-all-sorts>.

<sup>12</sup> *Id.*

<sup>13</sup> Michael Riley, *NSA Said to Exploit Heartbleed Bug for Intelligence for Years*, Bloomberg, Apr. 12, 2014, <http://www.bloomberg.com/news/2014-04-11/nsa-said-to-have-used-heartbleed-bug-exposing-consumers.html>.

<sup>14</sup> The Obama Administration refuted a Bloomberg News report published on the website of the Office of the Director of National Intelligence. See ODNI, Statement on Bloomberg News Story, *supra* note 1.

<sup>15</sup> *Id.*

<sup>16</sup> *Id.* Other disclosures have referred to the Administration’s review of the Vulnerabilities Equities Process. On April 13, a spokesperson for the President’s National Security Council told reporters that a three-month review of Committee’s recommendations had concluded and resulted in an interagency process to evaluate the value of disclosure when a security flaw is discovered against the value of keeping the discovery secret for later use by the intelligence community. Gautham Nagesh, *Heartbleed Sheds Light on NSA’s Use of Bugs*, Wall St. J. Tech., Apr. 13, 2014, 3:07 PM, <http://online.wsj.com/news/articles/SB10001424052702303887804579499801713379952>. During his confirmation hearing as director of the NSA and Cyber Command, Vice Admiral Michael Rogers previously stated that, within the NSA, “there is a mature and efficient equities resolution process for handling ‘0-day’ vulnerabilities discovered in any commercial product or system (not just software) utilized by the U.S. and its allies.” Kim Zetter, *Obama: NSA Must Reveal Bugs Like Heartbleed, Unless They Help the NSA*, Wired,



According to its April 11 statement, the White House initiated a review of its zero-day policies in response to the Review Committee's final report and recommendations.<sup>17</sup> It had concluded that the "Vulnerabilities Equities Process," the process by which agencies decide when to disclose and when to conceal a discovered software vulnerability, would need to be "reinvigorated" in order to address the Committee's concerns. This "reinvigorated" process established a "bias"<sup>18</sup> or a "default"<sup>19</sup> in favor of disclosure that is reportedly embodied in a presidential directive.<sup>20</sup> Apparently exempt from the directive's presumption of disclosure are vulnerabilities presenting "a clear national security or law enforcement need."<sup>21</sup> The directive does not appear to address security vulnerabilities or exploits bought and paid for by government agencies.<sup>22</sup>

### III. The Requested Records

Accordingly, the ACLU seeks disclosure of the following records:

1. The presidential guidance and/or directive concerning the discovery, disclosure, non-disclosure, or use of security vulnerabilities, as discussed above and as referenced by the April 11 statement by the Office of the Director of National Intelligence.

---

Apr. 4, 2014, 6:30 AM, <http://www.wired.com/2014/04/obama-zero-day>. The Administration followed up these statements with a blog explaining the factors that the government may weigh when determining whether to disclose a vulnerability. See Michael Daniel, *Heartbleed: Understanding When We Disclose Cyber Vulnerabilities*, White House Blog, Apr. 28, 2014 3:00 PM, <http://www.whitehouse.gov/blog/2014/04/28/heartbleedunderstanding-when-we-disclose-cyber-vulnerabilities>.

<sup>17</sup> ODNI, Statement on Bloomberg News Story, *supra* note 1.

<sup>18</sup> Nagesh, *Heartbleed Sheds Light*, *supra* note 16 (quoting NSC Spokesperson Hayden as saying, "[t]his process is biased toward responsibly disclosing such vulnerabilities.").

<sup>19</sup> Zetter, *Obama: NSA Must Reveal Bugs*, *supra* note 16 (attributing current NSA Director Rogers with the statement that "the default is to disclose vulnerabilities in products and systems used by the U.S. and its allies").

<sup>20</sup> See Riley, *Trove of Software Flaws Used by U.S.*, *supra* note 2. The presidential directive also appears to require technical experts to describe vulnerabilities in detail and proffer proposals for disclosure. In addition, statements indicate that the directive implements a new interagency adjudicatory process for reviewing technicians' determinations against the default of disclosure. See Zetter, *Obama: NSA Must Reveal Bugs*, *supra* note 16.

<sup>21</sup> David E. Sanger, *Obama Lets N.S.A. Exploit Some Internet Flaws, Officials Say*, N.Y. Times, Apr. 12, 2014, <http://www.nytimes.com/2014/04/13/us/politics/obama-lets-nsa-exploit-some-internet-flaws-officials-say.html>.

<sup>22</sup> Zetter, *Obama: NSA Must Reveal Bugs*, *supra* note 16 (noting that "[t]he statement by the Office of the Director of National Intelligence about the new bias toward disclosure . . . doesn't mention vulnerabilities discovered and sold to the government by contractors, zero-day brokers or individual researchers, some of whom may insist in their sale agreements that the vulnerability not be disclosed.").

2. Any policies, guidance, and/or directives concerning government purchase of security vulnerabilities or exploits, and government disclosure, non-disclosure, or use of purchased vulnerabilities or exploits.
3. Any policies, guidance, and/or directives concerning intra-agency or interagency reporting of security vulnerabilities or exploits, whether discovered or purchased by the government.
4. Any records and/or reports concerning actual government disclosures of security vulnerabilities to the companies, organizations, programmers, or developers responsible for maintaining the vulnerable software.

AMERICAN CIVIL LIBERTIES  
UNION FOUNDATION

This category of records should be construed broadly and to include all records and reports regarding the number and frequency of vulnerability disclosures; the number and frequency of communications regarding each disclosure; the disclosures; the nature and severity of each disclosed vulnerability; and the software affected.

The ACLU requests that this agency process and release documents on a rolling basis, and in the order in which requested categories of documents are listed above; *i.e.*, by prioritizing release of the presidential guidance and/or directive concerning disclosure of discovered vulnerabilities; then documents concerning the purchase of security vulnerabilities or exploits; then documents concerning intra- and interagency reporting of security vulnerabilities; and finally, documents recording and reporting actual vulnerabilities disclosures.

The ACLU requests that responsive electronic records be provided electronically in their native file format. *See* 5 U.S.C. § 552(a)(3)(B). If this FOIA request is denied in whole or in part, the ACLU requests disclosure of the reasons for each denial, pursuant to 5 U.S.C. § 552(a)(6)(A)(i). In addition, the ACLU requests release of all segregable portions of otherwise exempt material, in accordance with 5 U.S.C. § 552(b).

#### **IV. Expedited Processing**

The ACLU requests expedited processing pursuant to 5 U.S.C. § 552(a)(6)(E). There is a "compelling need" for expeditious disclosure because the documents requested are urgently needed by an organization primarily engaged in disseminating information in order to inform the public about actual or alleged government activity. 5 U.S.C. § 552(a)(6)(E)(v). In addition, there is an "urgency to inform the public" concerning the requested records, 28 C.F.R. § 16.5(d)(ii), because the records relate to a "breaking



news story of general public interest," 32 C.F.R. § 286.4(d)(3), (d)(3)(ii) & (d)(3)(ii)(A); *Open Am. v. Watergate Spec. Prosec. Force*, 547 F.2d 605, 614 (D.C. Cir. 1976) (recognizing right of expedition).

News media continue to report developments on the "Heartbleed" vulnerability and its widespread impact. Data thefts leveraged against the "Heartbleed" vulnerability were followed by speculation that undisclosed breaches may vastly exceed those initially reported incidents.<sup>23</sup> Hundreds of thousands of websites appear to have been rendered vulnerable to the "Heartbleed" threat,<sup>24</sup> the nature of which is evolving.<sup>25</sup>

Government response to the zero-day threat, moreover, has become a major news story in its own right.<sup>26</sup> On April 14, the Canadian tax authority reported the loss of hundreds of taxpayers' identity information to attacks on government websites.<sup>27</sup> By April 20, the Department of Health and Human Services had recalled as many as eight million user passwords to its online insurance exchange Healthcare.gov.<sup>28</sup> The Department of Homeland Security issued a public service announcement urging Americans to change their passwords and to monitor their social media, email, and bank accounts for irregular activity.<sup>29</sup>

AMERICAN CIVIL LIBERTIES  
UNION FOUNDATION

<sup>23</sup> Peter Eckersley, *Wild at Heart: Were Intelligence Agencies Using Heartbleed in November 2013?* Electronic Frontier Found., Apr. 10, 2014, <https://www.eff.org/deeplinks/2014/04/wild-heart-were-intelligence-agencies-using-heartbleed-november-2013>.

<sup>24</sup> See, e.g., Paul Mutton, *Half a Million Widely Trusted Websites Vulnerable to Heartbleed Bug*, Netcraft, Apr. 8, 2014, <http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html>.

<sup>25</sup> See, e.g., Brian Fung, *Heartbleed Is About to Get Worse, And It Will Slow the Internet to a Crawl*, Wash. Post Switch Blog, Apr. 14, 2014, 2:54 PM, <http://www.washingtonpost.com/blogs/the-switch/wp/2014/04/14/heartbleed-is-about-to-get-worse-and-it-will-slow-the-internet-to-a-crawl/> (reporting that "Heartbleed"-based thefts of credentials known as "security certificates" for popular websites like Google.com could be used to develop "fake" websites, exposing computers to all variety of cyber attacks).

<sup>26</sup> The collateral damage associated with exploiting, rather than correcting, security vulnerabilities has become a topic of considerable debate. See, e.g., Menn, *U.S. Cyberwar Strategy Stokes Fear*, *supra* note 6 (describing growing concerns in the technology industry and intelligence community that "Washington is in effect encouraging hacking and failing to disclose to software companies and customers the vulnerabilities exploited by the purchased hacks.").

<sup>27</sup> Jim Finkle & Louise Egan, *'Heartbleed' Blamed in Attack on Canada Tax Agency, More Expected*, Reuters, Apr. 15, 2014, 4:01 AM, <http://in.reuters.com/article/2014/04/14/us-cybersecurity-heartbleed-canada-idinkbn0d00ld20140414>.

<sup>28</sup> David Murphy, *'Heartbleed' Exploit Forces Healthcare.gov to Reset User Passwords*, PC Mag, Apr. 20, 2014, 2:00 AM, <http://www.pcmag.com/article2/0,2817,2456825,00.asp>.

<sup>29</sup> Press Release, Larry Zelvin, Reaction on "Heartbleed": Working Together to Mitigate Cybersecurity Vulnerabilities, Nat'l Cybersecurity & Comm'ns Integration Ctr., Dep't of Homeland Security (Apr. 11, 2014), available at <https://www.dhs.gov/blog/2014/04/11/reaction-%E2%80%99Heartbleed%E2%80%99D-working-together-mitigate-cybersecurity-vulnerabilities-0>.

Expedited release of the requested records will allow the public to evaluate government policies on the purchase, exploitation, and disclosure of zero-day vulnerabilities in the context of the breaking "Heartbleed" news story. These policies have become central to a national debate concerning the risk and potential repercussions of the zero-day threat.<sup>30</sup>

## V. Limitation of Processing Fees

The ACLU requests a limitation of search and review fees as a "representative of the news media." 5 U.S.C. § 552(a)(4)(A)(ii)(II). The ACLU meets the statutory definition of a "representative of the news media" as an "entity that gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw materials into a distinct work, and distributes that work to an audience." 5 U.S.C. § 552(a)(4)(A)(ii).<sup>31</sup> Indeed, the ACLU recently was held to be a "representative of the news media" in court.<sup>32</sup>

AMERICAN CIVIL LIBERTIES  
UNION FOUNDATION

The American Civil Liberties Union is national organization working to protect civil rights and civil liberties. Dissemination of information about actual or alleged government activity is a critical and substantial component of the ACLU's work. Among other things, the ACLU is known for its advocacy of national security and surveillance policies that are consistent with the Constitution, the rule of law, and fundamental human rights. The ACLU also educates the public about U.S. national security and law-enforcement policies and practices respecting, among other issues, government transparency and accountability; cybersecurity and digital rights; privacy and domestic surveillance; and the social and human costs of national security programs.

A substantial part of the ACLU's work involves the use of records disclosed under the Freedom of Information Act to educate the press and public about the activities of government. Its regular means of disseminating and editorializing information obtained through FOIA requests include a paper newsletter distributed to approximately 450,000 people; a bi-weekly electronic newsletter distributed to approximately 300,000 subscribers;

<sup>30</sup> Daniel, *Heartbleed: Understanding When We Disclose Cyber Vulnerabilities*, *supra* note 16.

<sup>31</sup> See also *Nat'l Sec. Archive v. Dep't of Def.*, 880 F.2d 1381, 1387 (D.C. Cir. 1989); cf. *Am. Civil Liberties Union v. Dep't of Justice*, 321 F. Supp. 2d 24, 29 n.5 (D.D.C. 2004) (finding non-profit public interest group to be "primarily engaged in disseminating information").

<sup>32</sup> *Serv. Women's Action Network v. Dep't of Defense*, 888 F. Supp. 2d 282, 287-88 (D. Conn. 2012); see also *Am. Civil Liberties Union of Wash. v. Dep't of Justice*, No. C09-0642RSL, 2011 WL 887731, at \*10 (W.D. Wash. Mar. 10, 2011) (finding ACLU of Washington to be a "representative of the news media"), *rec'd in part on other grounds*, 2011 WL 1900140 (W.D. Wash. May 19, 2011).



published reports, books, pamphlets, and fact sheets; a video series; a widely read blog; a popular Twitter feed; and a heavily visited website. The ACLU website features analyses of FOIA disclosures, links to released documents, and charts that gather, summarize, and present information obtained through FOIA. Additionally, the ACLU disseminates analysis to journalists and researchers through case-dedicated webpages, press releases and news briefings, and to students through "know your rights" publications, educational brochures, television series, and speaking engagements.

The ACLU makes FOIA information available to everyone, including tax-exempt organizations, not-for-profit groups, researchers, faculty members, law students, policy makers, reporters, and members of the general public for no cost or for a nominal fee. The ACLU makes archived materials available at the American Civil Liberties Union Archives at Princeton University Library.<sup>33</sup>

AMERICAN CIVIL LIBERTIES  
UNION FOUNDATION

## VI. Waiver of Costs

The ACLU also requests a waiver of all search, review, or duplication fees on the ground that disclosure of the requested information is in the public interest because it is "likely to contribute significantly to public understanding of the operations or activities of the government," and it is "not primarily in the commercial interest of the requester." 5 U.S.C. § 552(a)(4)(A)(iii). This request clearly satisfies these criteria.

There can be no doubt that the subject of the request is of significant interest to the American public. As discussed above, the government has characterized the threat of cyber attacks as one of the greatest threats facing the country.<sup>34</sup> Clearly, the process by which the government chooses to exploit zero-day vulnerabilities at the cost of decreased security from cyber attacks a matter of public interest and concern.

Disclosure of the zero-day directive and related policies will help the public to assess the adequacy of the procedures implementing the alleged "bias" for responsible disclosure. Disclosure of the requested documents will allow the public to evaluate whether the claimed exemptions conflict with the recommendation of the President's Review Committee that zero-day vulnerabilities be used only in those "rare instances" presenting intelligence requirements of a "urgent and significant national security priority."<sup>35</sup> Disclosure will let the public understand if agencies may bypass

<sup>33</sup> In addition to the national ACLU offices, there are fifty-three ACLU affiliate and national chapter offices located throughout the United States and Puerto Rico. These offices further disseminate ACLU material to local residents, schools, and organizations through a variety of means, including their own websites, publications, and newsletters.

<sup>34</sup> Menn, *U.S. Cyberwar Strategy*, *supra* note 6.

<sup>35</sup> Review Grp., *Liberty and Security in a Changing World*, *supra* note 7, at 219-20. Recommendation 30 urges that exploitation of zero-days be authorized only following "a

the disclosure bias by simply purchasing vulnerabilities or exploits from contractors, zero-day brokers, or individual researchers. Finally, disclosure will let the public know if the "bias" for disclosure is retroactive or if it applies only to zero-day vulnerabilities discovered or purchased after issuance of the President's zero-day directive.

The American Civil Liberties Union, a nonprofit organization, plans to disseminate to the public at no cost any documents disclosed in response to this request. As discussed above, disclosure to the ACLU will substantially increase the public impact of the agency's disclosure.

Thank you for your prompt attention to this matter. If the search and review fees are not waived, the ACLU asks that it be notified immediately at the email address listed below.

AMERICAN CIVIL LIBERTIES  
UNION FOUNDATION

Please furnish the requested records to:  
Rita Cant  
American Civil Liberties Union Foundation  
125 Broad Street, 18th Floor  
New York, NY 10004  
rcant@aclu.org

Sincerely,



Rita Cant  
Alex Abdo  
Nathan Freed Wessler  
Chris Soghoian  
Daniel K. Gillmor  
American Civil Liberties Union  
Speech, Privacy, and  
Technology Project  
125 Broad Street, 18th Floor  
New York, NY 10004  
(212) 549-2500

---

senior-level, interagency approval process that employs a risk-management approach" and involves "all appropriate departments"; and that authorizations be "temporar[y]" and as an alternative to "immediately fixing the underlying vulnerability." *Id.* at 220.