

Office of the Director of National Intelligence  
Washington, DC

FEB 04 2015

Ms. Ruth 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), that ODNI release information regarding the exploitation of "zero-day" vulnerabilities—security flaws that are unknown to the software's programme.

Your request was processed in accordance with the FOIA, as amended, 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 and 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 under the National Security Act of 1947, as amended, 50 U.S.C. § 3024(m)(1), which protects, among other things, the information of ODNI personnel; and
- (b)(6), which applies to information that would constitute an unwarranted invasion of the personal privacy of an individual.

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

You may appeal your determination within 45 days of receiving this letter by sending a written appeal letter, citing the basis of the appeal to the address below.

Office of the Director of National  
Information Management Office  
Washington, D.C.

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, DNI Division

Enclosure

**ENCLOSURE**

**1**



APR 30 2014



AMERICAN CIVIL LIBERTIES UNION

DE 2014 APR 30 11

Legal Department

FAX: (212) 549-2

FAX TRANS

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

**FAX NUMBER:** (703) 87

**FROM:** Rita Cant, American Civil Liberties Union

**DATE:** April 29, 2014

**Total number of pages (including attachments):**



In this fax, please

This transmission is intended for the solo use of the individual and entity to whom it is addressed, and may contain information that is privileged, confidential and exempt from public release. The unauthorized disclosure or application of this transmission by someone other than the addressee or its designated agent is strictly prohibited.



www.aclu.org  
April 29, 2014

VIA FACSIMILE

Director of National Intelligence  
Information Management Division  
Attn: Jennifer L. Hudson  
Washington, D.C. 20505-1111 Fax: (703) 874-8910

National Security Agency / Special Source Operations  
NSP5 / FOIA Request 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

AMERICAN CIVIL LIBERTIES  
UNION FOUNDATION  
NATIONAL OFFICE  
NEW YORK, NY 10004-1100

Department of Justice  
FOIA/PA Mail Referral Unit  
Room 1100  
Washington, D.C. 20530-0001 Fax: (301) 541-0772

Office of Legal Counsel  
Attn: Elizabeth Farris  
Room 5515, 950 Pennsylvania Avenue, N.W.  
Washington, D.C. 20530-0001 Fax: (202) 514-0535

Federal Bureau of Investigation  
FOI/PA Request and Information Dissemination Section  
170 N. Market Street  
Winchester, VA 22602-4842 Fax: (540) 868-4201

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 1<sup>st</sup> Street, N.W.  
Washington, D.C. 20536-5009 Fax: (202) 1-200-4000



I. **Buy and Stockpile**

Zero-day vulnerabilities have been reported by security organizations 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, contents of email inboxes, and medical and bank account records, as well as commercial trade secrets and other proprietary information.<sup>5</sup>

For these reasons, zero-day vulnerabilities are sought by cyber criminals and governments alike.<sup>6</sup> When military, intelligence, and 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 buy and stockpile vulnerabilities. The Review Committee on Intelligence and Communication observed: "A vulnerability that can be exploited on the battlefield can be exploited elsewhere."

The Review Committee recently urged the White House to 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 vulnerabilities to software programmers would "strengthen[] the security of US Government critical infrastructure and other computer systems." 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 Embarrassing History of Cyberwar Attacks in the Real World*, Symantec Research Labs, Oct. 16, 2012, [http://users.eoc.cmu.edu/~tdumitras/public\\_documents/bilge12\\_zero\\_day.pdf](http://users.eoc.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>.

<sup>7</sup> Bits Blog, Apr. 2, 2011, [http://bits.blogs.nytimes.com/2011/04/02/the-rsa-did-it/?\\_php=true&\\_type=blogs&\\_r=0](http://bits.blogs.nytimes.com/2011/04/02/the-rsa-did-it/?_php=true&_type=blogs&_r=0).

<sup>8</sup> Review Grp. on Intelligence and Comm., *Report of the Review Group on Intelligence and Communications Activities* (2013), available at [http://www.whitehouse.gov/sites/default/files/omb/eo/13526/12-12\\_rpt\\_final\\_report.pdf](http://www.whitehouse.gov/sites/default/files/omb/eo/13526/12-12_rpt_final_report.pdf).

<sup>9</sup> *Id.* at 220.

<sup>10</sup> *Id.*





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. It had concluded that the "Vulnerabilities Equities Process," the process by which agencies decide whether and when to conceal a discovered software vulnerability, would need to be "reinvigorated" in order to address the Committee's concerns. This "reinvigorated" process establishes a presumption of disclosure of a vulnerability to a responsible individual 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>

AMERICAN CIVIL LIBERTIES  
UNION FOUNDATION

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 government must consider in deciding whether to disclose a vulnerability.

Danger, *Wired*, Apr. 4, 2014, 6:30 AM.

Blog, Apr. 28, 2014 3:00 PM,

<http://www.whitehouse.gov/blog/2014/04/28/clear-headed-understanding-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 [redacted] 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 "[redacted]... vulnerabilities in our deployed systems used by the NSA...").

<sup>20</sup> See *R. J.*

also appears to require technical experts to describe vulnerabilities in 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 Inter-*

*Times*, Apr. 11, 2014, <http://www.nytimes.com/2014/04/11/us/politics/obamas-lets-nsa-exploit-some-internet-flaws-officials-say.html>.

<sup>22</sup> Zetter, *Obama: NSA Must Reveal*

Office of the Director of National Intelligence 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 disclosed or originated by a government...

disclosures of security vulnerabilities to the companies, organizations, programmers, or developers responsible for maintaining the vulnerable software.

This category of records should be construed broadly and to include the frequency of vulnerability disclosures; the number and frequency of communications regarding the security of software affected.

The ACLU requests that this agency provide and release documents on a rolling basis, and in the order in which requested categories of documents are listed: first, documents concerning the purchase of security 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 a 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



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. Limit on Processing Fees

The ACLU is a "representative of the news media" and meets the statutory definition as an "entity that gathers information or potential information from the public, uses its editorial skills to turn the raw materials into a distinct work, and disseminates that work to an audience."<sup>31</sup> 5 U.S.C. § 552(a)(1)(A). Indeed, the ACLU recently was recognized as a "news media" in court.<sup>32</sup>

The American Civil Liberties Union is a national organization working to protect civil rights and civil liberties. Dissemination of information about a state or federal 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 law-enforcement policies and practices respecting, among other issues, government transparency and accountability; human 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 is through press releases distributed to approximately 45

<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 1351, 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. 10-0642RSL, 2011 WL 887731, at \*10 (W.D. Wash. Mar. 10, 2011) (finding ACLU of Washington a "news media" organization); *Am. Civil Liberties Union of Wash. v. Dep't of Justice*, 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 popular website. The ACLU website features analyses of FOIA disclosures, links to released documents, and charts that gather, organize, 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 organizations, faculty members, law students, policy makers, reporters, and members of the general public for no cost or for a nominal fee. The ACLU also has 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 costs of duplication for the requested information 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)(ii). This information is of significant interest to the American public.

There can be no doubt that the request is of significant interest to the American public. As discussed above, the government has characterized the request as a matter of national security for 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 information will allow the public to assess the efficacy of the procedures implementing the alleged "bias" for responsible disclosure. Disclosure of the requested documents will allow the public to determine whether the claim of 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 a general policy of

<sup>33</sup> In addition to the national ACLU offices, there are fifty-three ACLU state 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 vulnerable contractors, zero individual researchers will let the public know applicable issuer

The American to disseminate to this request. As discussed above, disclosure to the ACLU will substantially increase the public impact of the agency's

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 the email address listed below.

AMERICAN CIVIL UNION FOUNDATION

Rita Cant

American Civil Liberties Union Found

125 Broad Street, 18th

New York, NY 10004

rcant@aclu.org

Sincerely,



Rita Cant

Alex Abdo

Nat

Chris Soghoian

Daniel K. Gillmor

ADVISOR ON 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 involve alternative to "immediately fixing the underlying vulnerability." *Id.* at 20.