Andrew Crocker (SBN 291596)
andrew@eff.org
Mark Rumold (SBN 279060)
mark@eff.org
Nathan Cardozo (SBN 259097)
nate@eff.org
ELECTRONIC FRONTIER FOUNDATION
815 Eddy St.
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993

Attorneys for Plaintiff
ELECTRONIC FRONTIER FOUNDATION

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

ELECTRONIC FRONTIER FOUNDATION, Plaintiff, v. NATIONAL SECURITY AGENCY, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE Defendants.	**COMPLAINT FOR INJUNCTIVE RELIEF FOR VIOLATION OF THE FREEDOM OF INFORMATION ACT, 5 U.S.C. § 552**

1. This is an action under the Freedom of Information Act (FOIA), 5 U.S.C. § 552, for injunctive and other appropriate relief. Plaintiff seeks the expedited processing and release of requested records in the possession of the National Security Agency (NSA) and the Office of the Director of National Intelligence (ODNI) describing the principles used by the government in deciding whether to disclose computer security flaws, a process sometimes referred to as the "Vulnerabilities Equity Process." The requested records concern a matter about which there is "[an] urgency to inform the public concerning actual or alleged federal government activity," and were "made by a person primarily engaged in disseminating information." 5 U.S.C. § 552(a)(6)(E)(v)(II); *see also* 32 C.F.R. § 299.5(f)(2); 32 C.F.R. § 1700.12. Therefore, Plaintiff is statutorily entitled to the immediate processing and release of the records it seeks.

PARTIES

2. Plaintiff Electronic Frontier Foundation (EFF) is a not-for-profit corporation established under the laws of the Commonwealth of Massachusetts, with offices in San Francisco, California and Washington, D.C. EFF is a donor-supported membership organization that works to inform policymakers and the general public about civil liberties issues related to technology and to act as a defender of those liberties. In support of its mission, EFF uses the FOIA to obtain and disseminate information concerning the activities of federal agencies.

3. Defendant National Security Agency (NSA) is a component of the Department of Defense, which is part of the Executive Branch of the United States Government. NSA is an "agency" within the meaning of 5 U.S.C. § 552(f)(1).

4. Defendant the Office of the Director of National Intelligence (ODNI) is a component of the Executive Branch of the United States Government. ODNI is an "agency" within the meaning of 5 U.S.C. § 552(f)(1).

JURISDICTION

5. This Court has both subject matter jurisdiction over this action and personal jurisdiction over the parties pursuant to 5 U.S.C. §§ 552(a)(4)(B) and 552(a)(6)(C)(i). This Court also has jurisdiction over this action pursuant to 28 U.S.C. § 1331.

VENUE AND INTRADISTRICT ASSIGNMENT

6. Venue is proper in this district under 5 U.S.C. § 552(a)(4)(B) and 28 U.S.C. § 1391(e).

7. Assignment to the San Francisco division is proper pursuant to Local Rule 3-2(c) and (d) because a substantial portion of the events giving rise to this action occurred in this district and division, where Plaintiff is headquartered.

//

//

//

//

//

FACTUAL ALLEGATIONS

Software Vulnerabilities and the Government's Use of Zero Days

8. In the past year, the American public, the press, and the United States government have been engaged in a significant, far-ranging public discussion of the government's intelligence gathering techniques and policies.

9. Part of that public debate has focused on the government's use of "zero days" (sometimes referred to as 0-days). Zero days are software flaws or vulnerabilities that allow an attacker with knowledge of the zero day to exploit it to gain access to computer systems, compromise security, intercept sensitive information, or otherwise exploit the software's weakness. They are so named because the software developer has had no time and hence no opportunity to resolve or patch the flaw.

10. A thriving market for vulnerabilities has developed, in which many actors, including agencies of the United States government, as well as foreign governments, purchase zero days.[1] Sales in this market typically require the seller to refrain from disclosure of the vulnerability to third parties. It is then up to the purchaser to determine whether and how to take advantage of the vulnerability information.

11. In December 2013, the Review Group on Intelligence and Communications Technologies—appointed by President Obama to assess the government's foreign intelligence activities—released a report recommending that the government clarify its policy with regard to disclosure of zero days: "US policy should generally move to ensure that Zero Days are quickly blocked, so that the underlying vulnerabilities are patched on US Government and other networks. In rare instances, US policy may briefly authorize using a Zero Day for high priority intelligence

[1] Nicole Perlroth & David E. Sanger, *Nations Buying as Hackers Sell Flaws in Computer Code*, N.Y. Times (July 14, 2013), http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html; Andy Greenberg, *Meet the Hackers Who Sell Spies the Tools to Crack Your PC (and Get Paid Six Figure Fees)*, Forbes (March 21, 2012), http://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees.

collection, following senior, interagency review involving all appropriate departments."[2]

"Heartbleed" and the Vulnerabilities Equities Process

12. In spring of 2014, computer security researchers announced discovery of a long-standing flaw in the popular open-source cryptographic library OpenSSL, which includes an implementation of the Transport Layer Security ("TLS") protocol. The flaw, known as "Heartbleed," allowed attackers to connect to servers using OpenSSL and cause the server to leak stored information, including passwords and other private information. Due to the importance of OpenSSL and the magnitude of the vulnerability, Heartbleed may have potentially "catastrophic" results for Internet security.[3]

13. On April 12, 2014, Bloomberg News published a story alleging that the NSA had prior knowledge of Heartbleed, and that the Agency had secretly exploited the vulnerability for intelligence gathering purposes for at least two years.[4]

14. The ODNI quickly denied that any part of the government knew about Heartbleed before April 2014. It further explained that in response to recommendations by the White House Review Group, the executive branch had "reviewed its policies in this area and reinvigorated an interagency process for deciding when to share vulnerabilities. This process is called the Vulnerabilities Equities Process."[5]

15. A subsequent blog post by the White House Cybersecurity Coordinator explained that the government, including the NSA, had "established principles to guide agency decision-making" including "a disciplined, rigorous and high-level decision-making process for

[2] President's Review Grp. on Intelligence and Commc'ns Tech., *Liberty and Security in a Changing World* at 219 (Dec. 12, 2013), http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[3] Yan Zhu, *Why the Web Needs Perfect Forward Secrecy More Than Ever*, Elec. Frontier Found. (Apr. 8, 2014), https://www.eff.org/deeplinks/2014/04/why-web-needs-perfect-forward-secrecy.

[4] Michael Riley, *NSA Said to Exploit Heartbleed Bug for Intelligence for Years*, Bloomberg (Apr. 11, 2014), http://www.bloomberg.com/news/2014-04-11/nsa-said-to-have-used-heartbleed-bug-exposing-consumers.html.

[5] 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://icontherecord.tumblr.com/post/82416436703/statement-on-bloomberg-news-story-that-nsa-knew.

vulnerability disclosure."[6]

Plaintiff's FOIA Request and Request for Expedited Processing

16. In a written FOIA request dated May 6, 2014 and sent by facsimile to the ODNI and the NSA on that day, Plaintiff requested from both agencies all records, including electronic records concerning or reflecting:

> "the development or implementation of the 'Vulnerabilities Equity Process' and . . . the 'principles' that guide the agency 'decision-making process for vulnerability disclosure' in the process described in the White House blog post."

17. In its May 6 correspondence, Plaintiff also formally requested that the processing of the FOIA request be expedited because it pertains to information about which there is "[an] urgency to inform the public concerning actual or alleged federal government activity," and were "made by a person primarily engaged in disseminating information." 5 U.S.C. § 552(a)(6)(E)(v)(II); *see also* 32 C.F.R. § 299.5(f)(2); 32 C.F.R. § 1700.12.

18. Defendant ODNI acknowledged Plaintiff's request via letter dated May 7, 2014. The letter noted ODNI's receipt of Plaintiff's request and granted Plaintiff's request for expedited processing.

19. Defendant NSA acknowledged Plaintiff's request via letter dated May 13, 2014. The letter noted NSA's acceptance of Plaintiff's request but denied Plaintiff's request for expedited processing.

20. By letter dated June 9, 2014 and sent by mail, Plaintiff appealed Defendant NSA's denial of expedited processing of Plaintiff's request, noting that ODNI had granted that same request.

21. Defendant NSA acknowledged receiving Plaintiff's administrative appeal via letter dated June 19, 2014. To date, Defendant NSA has not informed Plaintiff of the outcome of the appeal.

[6] Michael Daniel, *Heartbleed: Understanding When We Disclose Cyber Vulnerabilities*, White House (Apr. 28, 2014), http://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities.

22. To date, Defendants have not produced any documents in response to Plaintiff's request described in paragraph 17, nor informed Plaintiff of an anticipated date for the completion of the processing of the request.

23. Not only have Defendants failed to expedite the processing of Plaintiff's request, but they have also exceeded the generally applicable twenty-day deadline for the processing of any FOIA request.

24. Plaintiff has exhausted the applicable administrative remedies with respect to the FOIA request referenced herein.

25. Defendants have wrongfully withheld the requested records from Plaintiff.

CAUSES OF ACTION

Violation of the Freedom of Information Act for Failure to Expedite Processing

26. Plaintiff repeats and realleges paragraphs 1-25.

27. Defendants have violated the FOIA by failing to expedite the processing of Plaintiff's FOIA request and release of the requested agency records.

28. Plaintiff is entitled to injunctive relief with respect to the expedited processing and release of the requested agency records.

Violation of the Freedom of Information Act for Wrongful Withholding of Agency Records

29. Plaintiff repeats and realleges paragraphs 1-25.

30. Defendants have wrongfully withheld agency records requested by Plaintiff by failing to comply with the statutory time limit for the processing of FOIA requests.

31. Plaintiff has exhausted the applicable administrative remedies with respect to Defendants' wrongful withholding of the requested records.

32. Plaintiff is entitled to injunctive relief with respect to the release and disclosure of the requested documents.

//

//

//

REQUESTED RELIEF

WHEREFORE, Plaintiff prays that this Court:

1. order Defendants and their components to immediately process the requested records in their entirety;
2. order Defendants and their components, upon completion of such expedited processing, to disclose the requested records in their entirety and make copies available to Plaintiff;
3. provide for expeditious proceedings in this action;
4. award Plaintiff its costs and reasonable attorneys fees incurred in this action; and
5. grant such other relief as the Court may deem just and proper.

DATED: July 1, 2014

By /s/ Andrew Crocker
Andrew Crocker

Mark Rumold
Nathan Cardozo
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109

Attorneys for Plaintiff
ELECTRONIC FRONTIER FOUNDATION