

ORAL ARGUMENT NOT YET SCHEDULED**Court of Appeals No. 14-5174**

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

FREEDOM WATCH, INC.,
Plaintiff-Appellant,

v.

DEPARTMENT OF STATE,
Defendant-Appellee.

APPEAL FROM AN ORDER
OF THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA
IN CIVIL CASE NO. 1:12-cv-01088

JOINT APPENDIX

LARRY KLAYMAN
Freedom Watch, Inc.
2020 Pennsylvania Ave. NW, Suite 345
Washington, DC 20006
Tel: (310) 595-0800
Email: leklayman@gmail.com

Attorney for Plaintiff-Appellant

JOYCE C. BRANDA
Acting Assistant Attorney General
RONALD C. MACHEN, JR.
United States Attorney

MATTHEW M. COLLETTE
CATHERINE H. DORSEY
(202) 514-3469
Attorneys, Appellate Staff
Civil Division, Room 7236
U.S. Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530-0001

Attorneys for Defendants-Appellees

INDEX TO JOINT APPENDIX

<u>Item</u>	<u>Page</u>
District Court Docket Sheet.....	1-6
Complaint (ECF No. 1).....	7-26
Materials from Defendants' Motion for Judgment on the Pleadings:	
Phillips Declaration (ECF No. 4-1).....	27-46
Meeks Declaration (ECF No. 4-2).....	47-67
Walter Declaration (ECF No. 4-3).....	68-87
Tidd Declaration (ECF No. 4-4).....	88-112
Court's Order of December 13, 2012 (ECF No. 8).....	113-114
Court's Order of December 18, 2012 (ECF No. 10).....	115
Materials from Defendants' Motion for Summary Judgment:	
State's Supplemental Declaration (ECF No. 11-1).....	116-123
Exhibit 3 to State's Supplemental Declaration (ECF No. 11-1).....	124-125
Exhibit 4 to State's Supplemental Declaration (ECF No. 11-1).....	126-127
Materials From Plaintiff's Opposition to Motion For Summary Judgment:	
Rule 56(d) Affidavit of Larry Klayman (ECF No. 13-1).....	128-129
Materials From Defendants' Reply in Support of Motion For Summary Judgment:	
State's Second Supplemental Declaration (ECF No. 23-1).....	130-150
Order Granting Summary Judgment (ECF No. 24).....	151
Memorandum Opinion Granting Summary Judgment (ECF No. 25).....	152-162
Notice of Appeal (ECF No. 26).....	163-164
Certificate of Service.....	165

U.S. District Court
District of Columbia (Washington, DC)
CIVIL DOCKET FOR CASE #: 1:12-cv-01088-CRC

FREEDOM WATCH, INC. v. NATIONAL SECURITY
AGENCY et al
Assigned to: Judge Christopher R. Cooper
Case in other court: USCA, 14-05174
Cause: 05:552 Freedom of Information Act

Date Filed: 06/28/2012
Jury Demand: None
Nature of Suit: 895 Freedom of
Information Act
Jurisdiction: U.S. Government Defendant

Plaintiff

FREEDOM WATCH, INC.

represented by Larry E. Klayman
LAW OFFICES OF LARRY
KLAYMAN
2020 Pennsylvania Avenue, NW
Suite 345
Washington, DC 20006
(310) 595-0800
Fax: (310) 275-3276
Email: leklayman@gmail.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

V.

Defendant

NATIONAL SECURITY AGENCY

represented by John Kenneth Theis
U.S. DEPARTMENT OF JUSTICE
P.O. Box 883
Washington, DC 20044
(202) 305-7632
Fax: (202) 616-8460
Email: john.k.theis@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph Charles Folio , III
U.S. DEPARTMENT OF JUSTICE
Civil Division
20 Massachusetts Avenue, NW
Room 7218
Washington, DC 20530
(202) 305-4968
Fax: (202) 616-8470
Email: Joseph.Folio@usdoj.gov
LEAD ATTORNEY

Defendant

CENTRAL INTELLIGENCE AGENCY

represented by John Kenneth Theis
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph Charles Folio , III
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

DEPARTMENT OF STATE

represented by John Kenneth Theis
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph Charles Folio , III
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

FourthParty Plaintiff

DEPARTMENT OF DEFENSE

represented by John Kenneth Theis
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph Charles Folio , III
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Date Filed	#	Docket Text
06/28/2012	1	COMPLAINT against CENTRAL INTELLIGENCE AGENCY, DEPARTMENT OF DEFENSE, DEPARTMENT OF STATE, NATIONAL SECURITY AGENCY (Filing fee \$ 350, receipt number 4616049678) filed by FREEDOM WATCH, INC.. (Attachments: # 1 Civil Cover Sheet)(jf,) . (Entered: 07/03/2012)
06/28/2012		SUMMONS (6) Issued as to CENTRAL INTELLIGENCE AGENCY, DEPARTMENT OF STATE, NATIONAL SECURITY AGENCY, DEPARTMENT OF DEFENSE, U.S. Attorney and U.S. Attorney General (jf,) (Entered: 07/03/2012)
08/30/2012	2	NOTICE of Appearance by John Kenneth Theis on behalf of CENTRAL INTELLIGENCE AGENCY, DEPARTMENT OF DEFENSE, DEPARTMENT OF STATE, NATIONAL SECURITY AGENCY (Theis, John) (Entered: 08/30/2012)

08/30/2012	3	ANSWER to 1 Complaint by CENTRAL INTELLIGENCE AGENCY, DEPARTMENT OF DEFENSE, DEPARTMENT OF STATE, NATIONAL SECURITY AGENCY.(Theis, John) (Entered: 08/30/2012)
09/05/2012		MINUTE ORDER: Before the Court in this FOIA case are a complaint and an answer. The requirements of LCvR 16.3 and Rule 26(f) of the Federal Rules of Civil procedure appear to be inapplicable. Defendant may have 30 days from the date of this order within which to file a dispositive motion or, in the alternative, to file a report setting forth the schedule according to which it will complete its production of documents to the plaintiff. Signed by Judge Robert L. Wilkins on 9/5/2012. (tcb) (Entered: 09/05/2012)
10/05/2012	4	MOTION for Judgment on the Pleadings , MOTION for Summary Judgment by CENTRAL INTELLIGENCE AGENCY, DEPARTMENT OF DEFENSE, DEPARTMENT OF STATE, NATIONAL SECURITY AGENCY (Attachments: # 1 Declaration, # 2 Declaration, # 3 Declaration, # 4 Declaration, # 5 Text of Proposed Order)(Theis, John) (Entered: 10/05/2012)
10/09/2012		MINUTE ORDER: The parties shall appear on December 10, 2012 in Courtroom 27A at 3:00 PM for a motions hearing on Defendants MOTION for Judgment on the Pleadings and MOTION for Summary Judgment. Signed by Judge Robert L. Wilkins on 10/9/2012. (tcb) (Entered: 10/09/2012)
10/24/2012	5	RESPONSE re 4 MOTION for Judgment on the Pleadings MOTION for Summary Judgment filed by FREEDOM WATCH, INC.. (Attachments: # 1 Exhibit David Sanger Article, # 2 Text of Proposed Order, # 3 Certificate of Service)(Klayman, Larry) (Entered: 10/24/2012)
11/05/2012	6	REPLY to opposition to motion re 4 MOTION for Judgment on the Pleadings MOTION for Summary Judgment filed by CENTRAL INTELLIGENCE AGENCY, DEPARTMENT OF DEFENSE, DEPARTMENT OF STATE, NATIONAL SECURITY AGENCY. (Theis, John) (Entered: 11/05/2012)
12/10/2012		Minute Entry for proceedings held before Judge Robert L. Wilkins: Motion Hearing held and concluded on 12/10/2012 re Defendant's 4 MOTION for Judgment on the Pleadings MOTION for Summary Judgment. Argument heard and Motion GRANTED in part and DENIED in part for reasons stated on the record in open court. The parties directed to meet and confer to submit a proposed order to the Court by close of business, Tuesday, December 11, 2012. Court further directed the parties to meet and confer regarding how to proceed in this case and file a joint status report with a proposed order attached by Monday, December 17, 2012. (Court Reporter Rebecca Stonestreet) (tcb) (Entered: 12/10/2012)
12/11/2012	7	NOTICE of Proposed Order by CENTRAL INTELLIGENCE AGENCY, DEPARTMENT OF DEFENSE, DEPARTMENT OF STATE, FREEDOM WATCH, INC., NATIONAL SECURITY AGENCY (Theis, John) (Entered: 12/11/2012)
12/13/2012	8	ORDER re: Defendants 4 Motion for Judgment on the Pleadings and Motion for Summary Judgment; it is hereby ORDERED that the Motion for Judgment on the Pleadings of Defendants National Security Agency and Central Intelligence Agency is GRANTED; and it is FURTHER ORDERED that Defendant

		Department of Defenses Motion for Partial Summary Judgment is GRANTED; and it is FURTHER ORDERED that Defendant Department of States Motion for Judgment on the Pleadings is GRANTED with respect to Request Numbers 1 and 3-6 of Plaintiffs Freedom of Information Act request; and it is FURTHER ORDERED that Defendant Department of States Motion for Judgment on the Pleadings is DENIED with respect to Request Number 2. Signed by Judge Robert L. Wilkins on 12/13/2012. (tcb) (Entered: 12/13/2012)
12/17/2012	9	STATUS REPORT by CENTRAL INTELLIGENCE AGENCY, DEPARTMENT OF DEFENSE, DEPARTMENT OF STATE, FREEDOM WATCH, INC., NATIONAL SECURITY AGENCY. (Attachments: # 1 Text of Proposed Order) (Theis, John) (Entered: 12/17/2012)
12/18/2012	10	ORDER: Upon consideration of the parties Joint Status Report (Dkt. No. 9), it is hereby ORDERED that no later than March 18, 2013, Defendant Department of State (State) will: (1) conclude its search for records responsive to Plaintiffs Request Number 2 that relate to the June 1, 2012 New York Times article, (2) process and produce any non-exempt records; and (3) produce a Vaughn index (to the extent one is required); and it is FURTHER ORDERED that State will then file a dispositive motion no later than April 17, 2013. Signed by Judge Robert L. Wilkins on 12/18/2012. (tcb) (Entered: 12/18/2012)
12/18/2012		Set/Reset Deadlines: Defendant Department of State (State) will: (1) conclude its search for records responsive to Plaintiffs Request Number 2 that relate to the June 1, 2012 New York Times article, (2) process and produce any non-exempt records; and (3) produce a Vaughn index (to the extent one is required) due by 3/18/2013.State Dispositive Motion due by 4/17/2013 (tcb) (Entered: 12/18/2012)
04/17/2013	11	MOTION for Summary Judgment by DEPARTMENT OF STATE (Attachments: # 1 Declaration, # 2 Text of Proposed Order)(Theis, John) (Entered: 04/17/2013)
04/30/2013	12	Unopposed MOTION for Extension of Time to File Response/Reply as to 11 MOTION for Summary Judgment by FREEDOM WATCH, INC. (Attachments: # 1 Text of Proposed Order, # 2 Certificate of Service)(Klayman, Larry) (Entered: 04/30/2013)
05/01/2013		MINUTE ORDER granting 12 Plaintiff's Motion for Extension of Time to File Response/Reply. Plaintiff shall file its response to Defendants' Motion for Summary Judgment by no later than May 20, 2013. Signed by Judge Robert L. Wilkins on 5/1/2013. (lrlw3) (Entered: 05/01/2013)
05/01/2013		Set/Reset Deadlines: Response to Motion for Summary Judgment due by 5/20/2013. (clv,) (Entered: 05/01/2013)
05/20/2013	13	RESPONSE re 11 MOTION for Summary Judgment filed by FREEDOM WATCH, INC.. (Attachments: # 1 Affidavit Rule 56(d) Affidavit of Larry Klayman)(Klayman, Larry) (Entered: 05/20/2013)
05/20/2013	14	NOTICE of Filing of Certificate of Service by FREEDOM WATCH, INC. re 13 Response to motion (Klayman, Larry) (Entered: 05/20/2013)
05/30/2013	15	MOTION for Extension of Time to File Response/Reply as to 11 MOTION for Summary Judgment by DEPARTMENT OF STATE (Attachments: # 1 Text of Proposed Order)(Theis, John) (Entered: 05/30/2013)

06/04/2013	16	RESPONSE re 15 MOTION for Extension of Time to File Response/Reply as to 11 MOTION for Summary Judgment and Request for Discovery filed by FREEDOM WATCH, INC.. (Attachments: # 1 Certificate of Service)(Klayman, Larry) (Entered: 06/04/2013)
06/05/2013	17	ORDER granting 15 MOTION for Extension of Time to File Response/Reply as to 11 MOTION for Summary Judgment ;It is hereby ORDERED that, by July 29,2013, Department of State shall file its reply in support of its Motion for Summary Judgment. Signed by Judge Robert L. Wilkins on 6/5/2013. (tcb) (Entered: 06/05/2013)
06/10/2013	18	MOTION for Discovery and To Shorten Time for Defendant to Respond by FREEDOM WATCH, INC. (Attachments: # 1 Certificate of Service, # 2 Text of Proposed Order)(Klayman, Larry) (Entered: 06/10/2013)
06/11/2013		MINUTE ORDER: It is hereby ORDERED that the Defendants are directed to file any response or opposition to Plaintiffs 18 MOTION for Discovery and To Shorten Time for Defendant to Respond by Monday, June 17, 2013 and any reply shall be due by no later than Wednesday, June 20, 2013. Signed by Judge Robert L. Wilkins on 6/11/2013. (tcb) (Entered: 06/11/2013)
06/14/2013	19	MOTION Expedited Ruling re Order, Set Deadlines,, by FREEDOM WATCH, INC. (Attachments: # 1 Exhibit Articles Showing State Department Cover Up, # 2 Certificate of Service)(Klayman, Larry) (Entered: 06/14/2013)
06/17/2013	20	RESPONSE re 18 MOTION for Discovery and To Shorten Time for Defendant to Respond filed by DEPARTMENT OF STATE. (Theis, John) (Entered: 06/17/2013)
06/18/2013		MINUTE ORDER: Plaintiffs MOTION Expedited Ruling re Order, Set Deadlines at DKT # 19 is hereby DENIED for failure to attach a proposed order pursuant to Local Rule 7(c) and failure to file a notice with required compliance with Local Rule 7(m). Signed by Judge Robert L. Wilkins on 6/18/2013. (tcb) (Entered: 06/18/2013)
06/18/2013		MINUTE ORDER: IT IS HEREBY ORDERED THAT Plaintiffs Motion to Take Discovery of State, Dkt. 18, is DENIED. The Court finds that Plaintiffs allegations of bad faith are speculative, and speculation accusations of bad faith do not entitle a FOIA plaintiff to discovery. Accuracy in Media, Inc. v. Natl Park Serv., 194 F.3d 120, 125 (D.C. Cir. 1999). If appropriate, Plaintiff can renew the motion after Defendant State Department has had the opportunity to fully explain the adequacy of its search for responsive records. Signed by Judge Robert L. Wilkins on 6/18/2013. (tcb) (Entered: 06/18/2013)
07/29/2013	21	Unopposed MOTION for Extension of Time to File Response/Reply as to 11 MOTION for Summary Judgment by DEPARTMENT OF STATE (Attachments: # 1 Text of Proposed Order)(Theis, John) (Entered: 07/29/2013)
07/30/2013	22	ORDER granting 21 Unopposed MOTION for Extension of Time to File Response/Reply as to 11 MOTION for Summary Judgment ; It is hereby ORDERED that, by July 30, 2013, Department of State shall file its reply in support of its Motion for Summary Judgment. Signed by Judge Robert L. Wilkins on 7/30/2013. (tcb) (Entered: 07/30/2013)
07/30/2013	23	REPLY to opposition to motion re 11 MOTION for Summary Judgment filed by

		DEPARTMENT OF STATE (Attachments: # <u>1</u> Declaration)(Thoms, John) (Entered: 07/30/2013)
01/24/2014		Case reassigned to the Calendar Committee who will oversee it until it is reassigned to another judge. Judge Robert L. Wilkins has been elevated to the U.S. Court of Appeals for DC and is no longer assigned to the case. Any questions should be directed to Terri Barrett, formerly Judge Wilkins deputy clerk, at 202-354-3179 or terri_barrett@dcd.uscourts.gov (tcb) (Entered: 01/24/2014)
04/07/2014		Case directly reassigned to Judge Christopher R. Cooper. Calendar Committee no longer assigned to the case. (zgt,) (Entered: 04/07/2014)
06/12/2014	24	ORDER granting 11 Motion for Summary Judgment. Signed by Judge Christopher R. Cooper on 6/12/2014. (lcrc1,) (Entered: 06/12/2014)
06/12/2014	25	MEMORANDUM OPINION re: 11 Defendant's Motion for Summary Judgment. Signed by Judge Christopher R. Cooper on 6/12/2014. (lcrc1,) . (Entered: 06/12/2014)
07/14/2014	26	NOTICE OF APPEAL TO DC CIRCUIT COURT as to 24 Order on Motion for Summary Judgment, 25 Order by FREEDOM WATCH, INC.. Filing fee \$ 505, receipt number 0090-3778370. Fee Status: Fee Paid. Parties have been notified. (Klayman, Larry) (Entered: 07/14/2014)
07/15/2014	27	Transmission of the Notice of Appeal, Order Appealed, and Docket Sheet to US Court of Appeals. The Court of Appeals fee was paid this date 7/14/14 re 26 Notice of Appeal to DC Circuit Court. (td,) (Entered: 07/15/2014)
07/16/2014		USCA Case Number 14-5174 for 26 Notice of Appeal to DC Circuit Court filed by FREEDOM WATCH, INC.. (kb) (Entered: 07/16/2014)
10/20/2014	28	NOTICE of Appearance by Joseph Charles Folio, III on behalf of CENTRAL INTELLIGENCE AGENCY, DEPARTMENT OF DEFENSE, DEPARTMENT OF STATE, NATIONAL SECURITY AGENCY (Folio, Joseph) (Entered: 10/20/2014)

PACER Service Center			
Transaction Receipt			
12/29/2014 18:00:36			
PACER Login:	leklayman:3555863:0	Client Code:	
Description:	Docket Report	Search Criteria:	1:12-cv-01088-CRC
Billable Pages:	5	Cost:	0.50

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

FREEDOM WATCH, Inc.
2020 Pennsylvania Ave. NW, Suite 345
Washington, DC 20006

Plaintiff,

v.

NATIONAL SECURITY AGENCY
9800 Savage Road
Fort Meade, M.D. 20755

CENTRAL INTELLIGENCE AGENCY
Washington, D.C. 20505

DEPARTMENT OF DEFENSE
1400 Defense Pentagon
Washington, D.C. 20301-1400

DEPARTMENT OF STATE
2201 C Street NW
Washington, D.C. 20520

Defendants.

COMPLAINT

Plaintiff Freedom Watch, Inc. brings this action against the National Security Agency, the Central Intelligence Agency, the Department of Defense, and the Department of State, to compel compliance with the Freedom of Information Act, 5 U.S.C. § 552 ("FOIA"). As grounds therefor, Plaintiff alleges as follows.

JURISDICTION AND VENUE

1. The Court has jurisdiction over this action pursuant to 5 U.S.C. § 552(a)(4)(B) and 28 U.S.C. §1331. Venue is proper in this district pursuant to 28 U.S.C. §1391(e).

PARTIES

2. Plaintiff Freedom Watch is a non-profit, public interest foundation organized under the laws of the District of Columbia and having its principal place of business at 2020 Pennsylvania Ave., NW Suite 345, Washington, DC, 20006. Plaintiff seeks to promote openness within the federal government and their actions.
3. Defendants are agencies of the United States Government. Defendants have possession, custody, and control of records to which Plaintiff seeks access.

STATEMENT OF FACTS

4. On or about June 1, 2012 Plaintiff sent a FOIA request, via facsimile and the mail, to defendants seeking records about leaked information as set forth below and attached as Exhibit 1. Specifically, Plaintiff sought:

"...all correspondence, memoranda, documents, reports, records, statements, audits, lists of names, applications, diskettes, letters, expense logs and receipts, calendar or diary logs, facsimile logs, telephone records call sheets, tape recordings, video/movie recordings, notes, examinations, opinions, folders, files, books, manuals, pamphlets, forms, drawings, charts, photographs, electronic mail, and other documents and things (hereinafter, "information") that refer or relate to the following in any way, within ten (10) business days as set forth below:

- 1) Any and all information that refers or relates to the New York Times article entitled "Obama Order Sped Up Wave of Cyberattacks Against Iran" by David E. Sanger on Friday, June 1, 2012, and which information was provided and leaked to Mr. Sanger and the New York Times;
- 2) Any and all information that refers or relates in any way to information released to David E. Sanger and/or made available to him;
- 3) The names of the persons, employers and job titles, and addresses of those who "leaked" the above information to David E. Sanger

- 4) Communications with The White House and/or Office of the President and/or Vice President that refer or relate in any way to the "leaked" information and/or the reasons for "leaking" the information;
- 5) Any and all information that refer or relate to the decision to "leak" the above previously classified information;
- 6) Any and all information that refers or relates to government agencies deciding to investigate who "leaked" the above previously classified information."

(Exhibit 1)(Given the identical requests sent to all Defendants, only the page of FOIA requests for Defendants CIA, Dept. of Defense, and Dept. of State are included.)

5. Plaintiff requested a fee waiver and expedited processing in accordance with the procedures set forth under the regulations of each agency.
6. The records Plaintiff seeks are of urgent importance and are in the extreme public interest. The American people need to be informed expeditiously through disseminations by Freedom Watch of the requested records, as it affects their immediate well being, economically and otherwise.
7. Between June 11, 2012 and June 12, 2012 Plaintiff received letters through the mail from Defendants acknowledging receipt of Plaintiff's FOIA requests.
8. Pursuant to 5 U.S.C. § 552 (a)(6)(A) Defendant was required and failed to respond timely to Plaintiff's FOIA request.
9. As of the date of this Complaint, Defendants have failed to produce any records responsive to the request or demonstrate that the responsive records are exempt from production. Nor have they indicated whether or when any responsive records will be produced, nor has a fee waiver been granted. In sum, Defendants have failed to respond to the requests in any substantive manner.

10. Because Defendants failed to comply with the time limits set forth in 5 U.S.C. §552(a)(6)(C), Plaintiff is deemed to have exhausted any and all administrative remedies with respect of its FOIA request, pursuant to 5 U.S.C. § 552(a)(6)(C).

COUNT 1

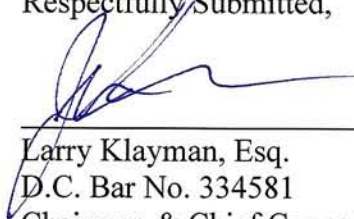
(Violation of FOIA, 5 U.S.C § 552, et. seq.)

11. Plaintiff realleges paragraphs 1 through 10 as if fully stated herein.
12. Defendants are unlawfully withholding records requested by Plaintiff pursuant to 5 U.S.C. § 552, et. seq.
13. Plaintiff is being irreparably harmed by reason of Defendants' unlawful withholding of requested records, and Plaintiff will continue to be irreparably harmed unless Defendants are compelled to conform to the requirements of this law.

WHEREFORE, Plaintiff respectfully requests that the Court: (1) Order Defendants to conduct expedited searches for any and all responsive records to Plaintiff's FOIA request and demonstrate that they employed search methods reasonably likely to lead to the discovery of records responsive to Plaintiff's FOIA request; (2) order Defendants to expeditiously produce, by a date certain, any and all records responsive to Plaintiff's FOIA request and a Vaughn index of any responsive records withheld under claim of exemption; (3) enjoin Defendants from continuing to withhold any and all records responsive to Plaintiff's FOIA request; (4) grant Plaintiff an award of attorney's fees and other litigation costs reasonably incurred in this action pursuant to 5 U.S.C. § 552(a)(4)(E); and (5) grant Plaintiff any other relief as the Court deems just or proper.

Dated: June 27, 2012

Respectfully Submitted,



Larry Klayman, Esq.
D.C. Bar No. 334581
Chairman & Chief Counsel
Freedom Watch
2020 Pennsylvania Ave. NW, Suite 345
Washington, DC 20006
Tel: (310) 595-0800
Email: leklayman@gmail.com

Exhibit 1



FREEDOM WATCH

▶ www.FreedomWatchUSA.org

▶ World Headquarters 2020 Pennsylvania Avenue, N.W., Suite 345, Washington, DC 20006-1811 ▶ (310) 595-0800 ▶ leklayman@gmail.com

Via Mail and Fax

June 1, 2012

National Security Agency
Attn: FOIA/PA Office (DJP4)
9800 Savage Road, Suite 6248
Ft. George G. Meade, MD 20755-6248

Re: Freedom of Information Act Request

Dear Sir/Madam:

On June 1, 2012, the New York Times published two articles, "Obama Order Sped Up Wave of Cyberattacks Against Iran" by David E. Sanger. This article, a copy of which is attached, relied in large part on previously classified information which was released by Obama administration sources on the President's behalf. This released information is thus no longer classified and is no longer exempt from being released pursuant to the Freedom of Information Act. 5 U.S.C. 552 et seq.

Pursuant to the Freedom of Information Act (5 U.S.C. § 552 et seq.), Freedom Watch requests that that the National Security Agency produce all correspondence, memoranda, documents, reports, records, statements, audits, lists of names, applications, diskettes, letters, expense logs and receipts, calendar or diary logs, facsimile logs, telephone records call sheets, tape recordings, video/movie recordings, notes, examinations, opinions, folders, files, books, manuals, pamphlets, forms, drawings, charts, photographs, electronic mail, and other documents and things (hereinafter, "information") that refer or relate to the following in any way, within ten (10) business days as set forth below:

- 1) Any and all information that refers or relates to the New York Times article entitled "Obama Order Sped Up Wave of Cyberattacks Against Iran" by David E. Sanger on Friday, June 1, 2012, and which information was provided and leaked to Mr. Sanger and the New York Times;
- 2) Any and all information that refers or relates in any way to information released to David E. Sanger and/or made available to him;

National Security Agency
FOIA Request
Page | 2

- 3) The names of the persons, employers and job titles, and addresses of those who “leaked” the above information to David E. Sanger
- 4) Communications with The White House and/or Office of the President and/or Vice President that refer or relate in any way to the “leaked” information and/or the reasons for “leaking” the information;
- 5) Any and all information that refer or relate to the decision to “leak” the above previously classified information;
- 6) Any and all information that refers or relates to government agencies deciding to investigate who “leaked” the above previously classified information.

If any responsive record or portion thereof is claimed to be exempt from production under FOIA, sufficient identifying information (with respect to each allegedly exempt record or portion thereof) must be provided to allow the assessment of the propriety of the claimed exemption. *Vaughn v. Rosen*, 484 F.2d 820 (D.C. Cir. 1973), *cert denied*, 415 U.S. 977 (1974). Additionally, pursuant to law, any reasonably segregable portion of a responsive record must be provided after redaction of any allegedly exempt material. 5 U.S.C. §552(b).

I request a waiver of all fees for this request under 5. U.S.C. § 552(a)(4)(A)(iii). Disclosure of the requested information to Freedom Watch is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in my commercial interest. The Islamic Republic of Iran's goal of obtaining nuclear weapons affects the safety of both Israel and the United States, thus putting American citizens at risk. Furthermore, the release of classified information by any particular individual within the executive branch, including the president, further endangers the American people and raises a spectre of corruption within the federal government that must be examined. Freedom Watch is engaged in the active dissemination of public information as is evident by our ongoing public interest legal work and continual fight against corruption within the United States government, and international cases, particularly with regard to Iran. Freedom Watch's website, freedomwatchusa.org serves as the primary means of disseminating that information, and is seen by millions of people annually. In addition, officials of Freedom Watch frequently appear on radio and television to disseminate important information to the public.

Furthermore, on behalf of Freedom Watch I am requesting expedited handling as provided in Department of Defense FOIA Regulation 54000.7-R because there is an urgency to inform the public about an actual or alleged federal government activity. Iran is reportedly on the verge of acquiring nuclear weapons and Israel is reportedly

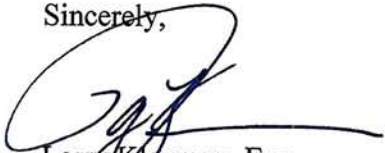
National Security Agency
FOIA Request
Page | 3

on the verge of attacking it to prevent their acquisition. The issue of a possible attack on Iran is of importance to the American people because Iran's acquiring of nuclear weapons places the safety of the American people as well as the safety of our allies in jeopardy. This war can break out any time because a strike is needed before Iran can gain the capability to build a bomb. This fact is also evidenced in the article mentioned above. There is an immediate clear and present danger to U.S. citizens, American military personnel.

The above mentioned "leaked" information is no longer in effect classified, if it ever was, as it was disclosed to the public by Mr. Sanger and The New York Times with the aid and complicity of President Obama and his administration. It was disclosed for political purposes to further President Obama's 2012 re-election campaign.

On behalf of Freedom Watch, I look forward to receiving the requested documents and a full fee waiver within ten (10) business days. You may have them delivered to the above address.

Sincerely,



Larry Klayman, Esq.
Chairman and General Counsel
2020 Pennsylvania Ave, N.W., Suite 345
Washington, D.C. 20006
leklayman@gmail.com

The New York Times

June 1, 2012

Obama Order Sped Up Wave of Cyberattacks Against Iran

By DAVID E. SANGER

WASHINGTON — From his first months in office, President Obama secretly ordered increasingly sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, significantly expanding America's first sustained use of cyberweapons, according to participants in the program.

Mr. Obama decided to accelerate the attacks — begun in the Bush administration and code-named Olympic Games — even after an element of the program accidentally became public in the summer of 2010 because of a programming error that allowed it to escape Iran's Natanz plant and sent it around the world on the Internet. Computer security experts who began studying the worm, which had been developed by the United States and Israel, gave it a name: Stuxnet.

At a tense meeting in the White House Situation Room within days of the worm's "escape," Mr. Obama, Vice President Joseph R. Biden Jr. and the director of the Central Intelligence Agency at the time, Leon E. Panetta, considered whether America's most ambitious attempt to slow the progress of Iran's nuclear efforts had been fatally compromised.

"Should we shut this thing down?" Mr. Obama asked, according to members of the president's national security team who were in the room.

Told it was unclear how much the Iranians knew about the code, and offered evidence that it was still causing havoc, Mr. Obama decided that the cyberattacks should proceed. In the following weeks, the Natanz plant was hit by a newer version of the computer worm, and then another after that. The last of that series of attacks, a few weeks after Stuxnet was detected around the world, temporarily took out nearly 1,000 of the 5,000 centrifuges Iran had spinning at the time to purify uranium.

This account of the American and Israeli effort to undermine the Iranian nuclear program is based on interviews over the past 18 months with current and former American, European and Israeli officials involved in the program, as well as a range of outside experts. None would allow

their names to be used because the effort remains highly classified, and parts of it continue to this day.

These officials gave differing assessments of how successful the sabotage program was in slowing Iran's progress toward developing the ability to build nuclear weapons. Internal Obama administration estimates say the effort was set back by 18 months to two years, but some experts inside and outside the government are more skeptical, noting that Iran's enrichment levels have steadily recovered, giving the country enough fuel today for five or more weapons, with additional enrichment.

Whether Iran is still trying to design and build a weapon is in dispute. The most recent United States intelligence estimate concludes that Iran suspended major parts of its weaponization effort after 2003, though there is evidence that some remnants of it continue.

Iran initially denied that its enrichment facilities had been hit by Stuxnet, then said it had found the worm and contained it. Last year, the nation announced that it had begun its own military cyberunit, and Brig. Gen. Gholamreza Jalali, the head of Iran's Passive Defense Organization, said that the Iranian military was prepared "to fight our enemies" in "cyberspace and Internet warfare." But there has been scant evidence that it has begun to strike back.

The United States government only recently acknowledged developing cyberweapons, and it has never admitted using them. There have been reports of one-time attacks against personal computers used by members of Al Qaeda, and of contemplated attacks against the computers that run air defense systems, including during the NATO-led air attack on Libya last year. But Olympic Games was of an entirely different type and sophistication.

It appears to be the first time the United States has repeatedly used cyberweapons to cripple another country's infrastructure, achieving, with computer code, what until then could be accomplished only by bombing a country or sending in agents to plant explosives. The code itself is 50 times as big as the typical computer worm, Carey Nachenberg, a vice president of Symantec, one of the many groups that have dissected the code, said at a symposium at Stanford University in April. Those forensic investigations into the inner workings of the code, while picking apart how it worked, came to no conclusions about who was responsible.

A similar process is now under way to figure out the origins of another cyberweapon called Flame that was recently discovered to have attacked the computers of Iranian officials, sweeping up information from those machines. But the computer code appears to be at least five years old, and American officials say that it was not part of Olympic Games. They have declined to say whether the United States was responsible for the Flame attack.

Mr. Obama, according to participants in the many Situation Room meetings on Olympic Games, was acutely aware that with every attack he was pushing the United States into new territory, much as his predecessors had with the first use of atomic weapons in the 1940s, of intercontinental missiles in the 1950s and of drones in the past decade. He repeatedly expressed concerns that any American acknowledgment that it was using cyberweapons — even under the most careful and limited circumstances — could enable other countries, terrorists or hackers to justify their own attacks.

“We discussed the irony, more than once,” one of his aides said. Another said that the administration was resistant to developing a “grand theory for a weapon whose possibilities they were still discovering.” Yet Mr. Obama concluded that when it came to stopping Iran, the United States had no other choice.

If Olympic Games failed, he told aides, there would be no time for sanctions and diplomacy with Iran to work. Israel could carry out a conventional military attack, prompting a conflict that could spread throughout the region.

A Bush Initiative

The impetus for Olympic Games dates from 2006, when President George W. Bush saw few good options in dealing with Iran. At the time, America’s European allies were divided about the cost that imposing sanctions on Iran would have on their own economies. Having falsely accused Saddam Hussein of reconstituting his nuclear program in Iraq, Mr. Bush had little credibility in publicly discussing another nation’s nuclear ambitions. The Iranians seemed to sense his vulnerability, and, frustrated by negotiations, they resumed enriching uranium at an underground site at Natanz, one whose existence had been exposed just three years before.

Iran’s president, Mahmoud Ahmadinejad, took reporters on a tour of the plant and described grand ambitions to install upward of 50,000 centrifuges. For a country with only one nuclear power reactor — whose fuel comes from Russia — to say that it needed fuel for its civilian nuclear program seemed dubious to Bush administration officials. They feared that the fuel could be used in another way besides providing power: to create a stockpile that could later be enriched to bomb-grade material if the Iranians made a political decision to do so.

Hawks in the Bush administration like Vice President Dick Cheney urged Mr. Bush to consider a military strike against the Iranian nuclear facilities before they could produce fuel suitable for a weapon. Several times, the administration reviewed military options and concluded that they would only further inflame a region already at war, and would have uncertain results.

For years the C.I.A. had introduced faulty parts and designs into Iran’s systems — even

tinkering with imported power supplies so that they would blow up — but the sabotage had had relatively little effect. General James E. Cartwright, who had established a small cyberoperation inside the United States Strategic Command, which is responsible for many of America’s nuclear forces, joined intelligence officials in presenting a radical new idea to Mr. Bush and his national security team. It involved a far more sophisticated cyberweapon than the United States had designed before.

The goal was to gain access to the Natanz plant’s industrial computer controls. That required leaping the electronic moat that cut the Natanz plant off from the Internet — called the air gap, because it physically separates the facility from the outside world. The computer code would invade the specialized computers that command the centrifuges.

The first stage in the effort was to develop a bit of computer code called a beacon that could be inserted into the computers, which were made by the German company Siemens and an Iranian manufacturer, to map their operations. The idea was to draw the equivalent of an electrical blueprint of the Natanz plant, to understand how the computers control the giant silvery centrifuges that spin at tremendous speeds. The connections were complex, and unless every circuit was understood, efforts to seize control of the centrifuges could fail.

Eventually the beacon would have to “phone home” — literally send a message back to the headquarters of the National Security Agency that would describe the structure and daily rhythms of the enrichment plant. Expectations for the plan were low; one participant said the goal was simply to “throw a little sand in the gears” and buy some time. Mr. Bush was skeptical, but lacking other options, he authorized the effort.

Breakthrough, Aided by Israel

It took months for the beacons to do their work and report home, complete with maps of the electronic directories of the controllers and what amounted to blueprints of how they were connected to the centrifuges deep underground.

Then the N.S.A. and a secret Israeli unit respected by American intelligence of cyberskills set to work developing the enormously complex computer worm that the attacker from within.

4 OPEN

MORE IN MI
Egypt A
Verdict
Read More

The unusually tight collaboration with Israel was driven by two imperatives. I. a part of its military, had technical expertise that rivaled the N.S.A.’s, and the Israelis had deep intelligence about operations at Natanz that would be vital to making the cyberattack a success. But American officials had another interest, to dissuade the Israelis from carrying out their own pre-emptive strike against the Iranian nuclear facilities. To do that, the Israelis would have to

be convinced that the new line of attack was working. The only way to convince them, several officials said in interviews, was to have them deeply involved in every aspect of the program.

Soon the two countries had developed a complex worm that the Americans called “the bug.” But the bug needed to be tested. So, under enormous secrecy, the United States began building replicas of Iran’s P-1 centrifuges, an aging, unreliable design that Iran purchased from Abdul Qadeer Khan, the Pakistani nuclear chief who had begun selling fuel-making technology on the black market. Fortunately for the United States, it already owned some P-1s, thanks to the Libyan dictator, Col. Muammar el-Qaddafi.

When Colonel Qaddafi gave up his nuclear weapons program in 2003, he turned over the centrifuges he had bought from the Pakistani nuclear ring, and they were placed in storage at a weapons laboratory in Tennessee. The military and intelligence officials overseeing Olympic Games borrowed some for what they termed “destructive testing,” essentially building a virtual replica of Natanz, but spreading the test over several of the Energy Department’s national laboratories to keep even the most trusted nuclear workers from figuring out what was afoot.

Those first small-scale tests were surprisingly successful: the bug invaded the computers, lurking for days or weeks, before sending instructions to speed them up or slow them down so suddenly that their delicate parts, spinning at supersonic speeds, self-destructed. After several false starts, it worked. One day, toward the end of Mr. Bush’s term, the rubble of a centrifuge was spread out on the conference table in the Situation Room, proof of the potential power of a cyberweapon. The worm was declared ready to test against the real target: Iran’s underground enrichment plant.

“Previous cyberattacks had effects limited to other computers,” Michael V. Hayden, the former chief of the C.I.A., said, declining to describe what he knew of these attacks when he was in office. “This is the first attack of a major nature in which a cyberattack was used to effect physical destruction,” rather than just slow another computer, or hack into it to steal data.

“Somebody crossed the Rubicon,” he said.

Getting the worm into Natanz, however, was no easy trick. The United States and Israel would have to rely on engineers, maintenance workers and others — both spies and unwitting accomplices — with physical access to the plant. “That was our holy grail,” one of the architects of the plan said. “It turns out there is always an idiot around who doesn’t think much about the thumb drive in their hand.”

In fact, thumb drives turned out to be critical in spreading the first variants of the computer worm; later, more sophisticated methods were developed to deliver the malicious code.

The first attacks were small, and when the centrifuges began spinning out of control in 2008, the Iranians were mystified about the cause, according to intercepts that the United States later picked up. “The thinking was that the Iranians would blame bad parts, or bad engineering, or just incompetence,” one of the architects of the early attack said.

The Iranians were confused partly because no two attacks were exactly alike. Moreover, the code would lurk inside the plant for weeks, recording normal operations; when it attacked, it sent signals to the Natanz control room indicating that everything downstairs was operating normally. “This may have been the most brilliant part of the code,” one American official said.

Later, word circulated through the International Atomic Energy Agency, the Vienna-based nuclear watchdog, that the Iranians had grown so distrustful of their own instruments that they had assigned people to sit in the plant and radio back what they saw.

“The intent was that the failures should make them feel they were stupid, which is what happened,” the participant in the attacks said. When a few centrifuges failed, the Iranians would close down whole “stands” that linked 164 machines, looking for signs of sabotage in all of them. “They overreacted,” one official said. “We soon discovered they fired people.”

Imagery recovered by nuclear inspectors from cameras at Natanz — which the nuclear agency uses to keep track of what happens between visits — showed the results. There was some evidence of wreckage, but it was clear that the Iranians had also carted away centrifuges that had previously appeared to be working well.

But by the time Mr. Bush left office, no wholesale destruction had been accomplished. Meeting with Mr. Obama in the White House days before his inauguration, Mr. Bush urged him to preserve two classified programs, Olympic Games and the drone program in Pakistan. Mr. Obama took Mr. Bush’s advice.

The Stuxnet Surprise

Mr. Obama came to office with an interest in cyberissues, but he had discussed them during the campaign mostly in terms of threats to personal privacy and the risks to infrastructure like the electrical grid and the air traffic control system. He commissioned a major study on how to improve America’s defenses and announced it with great fanfare in the East Room.

What he did not say then was that he was also learning the arts of cyberwar. The architects of Olympic Games would meet him in the Situation Room, often with what they called the “horse blanket,” a giant foldout schematic diagram of Iran’s nuclear production facilities. Mr. Obama authorized the attacks to continue, and every few weeks — certainly after a major attack — he

would get updates and authorize the next step. Sometimes it was a strike riskier and bolder than what had been tried previously.

“From his first days in office, he was deep into every step in slowing the Iranian program — the diplomacy, the sanctions, every major decision,” a senior administration official said. “And it’s safe to say that whatever other activity might have been under way was no exception to that rule.”

But the good luck did not last. In the summer of 2010, shortly after a new variant of the worm had been sent into Natanz, it became clear that the worm, which was never supposed to leave the Natanz machines, had broken free, like a zoo animal that found the keys to the cage. It fell to Mr. Panetta and two other crucial players in Olympic Games — General Cartwright, the vice chairman of the Joint Chiefs of Staff, and Michael J. Morell, the deputy director of the C.I.A. — to break the news to Mr. Obama and Mr. Biden.

An error in the code, they said, had led it to spread to an engineer’s computer when it was hooked up to the centrifuges. When the engineer left Natanz and connected the computer to the Internet, the American- and Israeli-made bug failed to recognize that its environment had changed. It began replicating itself all around the world. Suddenly, the code was exposed, though its intent would not be clear, at least to ordinary computer users.

“We think there was a modification done by the Israelis,” one of the briefers told the president, “and we don’t know if we were part of that activity.”

Mr. Obama, according to officials in the room, asked a series of questions, fearful that the code could do damage outside the plant. The answers came back in hedged terms. Mr. Biden fumed. “It’s got to be the Israelis,” he said. “They went too far.”

In fact, both the Israelis and the Americans had been aiming for a particular part of the centrifuge plant, a critical area whose loss, they had concluded, would set the Iranians back considerably. It is unclear who introduced the programming error.

The question facing Mr. Obama was whether the rest of Olympic Games was in jeopardy, now that a variant of the bug was replicating itself “in the wild,” where computer security experts can dissect it and figure out its purpose.

“I don’t think we have enough information,” Mr. Obama told the group that day, according to the officials. But in the meantime, he ordered that the cyberattacks continue. They were his best hope of disrupting the Iranian nuclear program unless economic sanctions began to bite harder and reduced Iran’s oil revenues.

Within a week, another version of the bug brought down just under 1,000 centrifuges. Olympic Games was still on.

A Weapon's Uncertain Future

American cyberattacks are not limited to Iran, but the focus of attention, as one administration official put it, “has been overwhelmingly on one country.” There is no reason to believe that will remain the case for long. Some officials question why the same techniques have not been used more aggressively against North Korea. Others see chances to disrupt Chinese military plans, forces in Syria on the way to suppress the uprising there, and Qaeda operations around the world. “We’ve considered a lot more attacks than we have gone ahead with,” one former intelligence official said.

Mr. Obama has repeatedly told his aides that there are risks to using — and particularly to overusing — the weapon. In fact, no country’s infrastructure is more dependent on computer systems, and thus more vulnerable to attack, than that of the United States. It is only a matter of time, most experts believe, before it becomes the target of the same kind of weapon that the Americans have used, secretly, against Iran.

This article is adapted from “Confront and Conceal: Obama’s Secret Wars and Surprising Use of American Power,” to be published by Crown on Tuesday.



FREEDOM WATCH

www.FreedomWatchUSA.org

World Headquarters 2020 Pennsylvania Avenue, N.W., Suite 345, Washington, DC 20006-1811 (310) 595-0800 leklayman@gmail.com

Via Mail and Fax

June 1, 2012

Office of Information Programs and Services
A/GIS/IPS/RL
U. S. Department of State
Washington, D. C. 20522-8100

Re: Freedom of Information Act Request

Dear Sir/Madam:

On June 1, 2012, the New York Times published two articles, "Obama Order Sped Up Wave of Cyberattacks Against Iran" by David E. Sanger. This article, a copy of which is attached, relied in large part on previously classified information which was released by Obama administration sources on the President's behalf. This released information is thus no longer classified and is no longer exempt from being released pursuant to the Freedom of Information Act. 5 U.S.C. 552 et seq.

Pursuant to the Freedom of Information Act (5 U.S.C. § 552 et seq.), Freedom Watch requests that that the Department of State produce all correspondence, memoranda, documents, reports, records, statements, audits, lists of names, applications, diskettes, letters, expense logs and receipts, calendar or diary logs, facsimile logs, telephone records call sheets, tape recordings, video/movie recordings, notes, examinations, opinions, folders, files, books, manuals, pamphlets, forms, drawings, charts, photographs, electronic mail, and other documents and things (hereinafter, "information") that refer or relate to the following in any way, within ten (10) business days as set forth below:

- 1) Any and all information that refers or relates to the New York Times article entitled "Obama Order Sped Up Wave of Cyberattacks Against Iran" by David E. Sanger on Friday, June 1, 2012, and which information was provided and leaked to Mr. Sanger and the New York Times;
- 2) Any and all information that refers or relates in any way to information released to David E. Sanger and/or made available to him;
- 3) The names of the persons, employers and job titles, and addresses of those who "leaked" the above information to David E. Sanger



FREEDOM WATCH

▶ www.FreedomWatchUSA.org

▶ World Headquarters 2020 Pennsylvania Avenue, N.W., Suite 345, Washington, DC 20006-1811 ▶ (310) 595-0800 ▶ leklayman@gmail.com

Via Mail and Fax

June 1, 2012

Information and Privacy Coordinator
Central Intelligence Agency
Washington, D.C. 20505

Re: Freedom of Information Act Request

Dear Sir/Madam:

On June 1, 2012, the New York Times published two articles, "Obama Order Sped Up Wave of Cyberattacks Against Iran" by David E. Sanger. This article, a copy of which is attached, relied in large part on previously classified information which was released by Obama administration sources on the President's behalf. This released information is thus no longer classified and is no longer exempt from being released pursuant to the Freedom of Information Act. 5 U.S.C. 552 et seq.

Pursuant to the Freedom of Information Act (5 U.S.C. § 552 et seq.), Freedom Watch requests that that the Central Intelligence Agency produce all correspondence, memoranda, documents, reports, records, statements, audits, lists of names, applications, diskettes, letters, expense logs and receipts, calendar or diary logs, facsimile logs, telephone records call sheets, tape recordings, video/movie recordings, notes, examinations, opinions, folders, files, books, manuals, pamphlets, forms, drawings, charts, photographs, electronic mail, and other documents and things (hereinafter, "information") that refer or relate to the following in any way, within ten (10) business days as set forth below:

- 1) Any and all information that refers or relates to the New York Times article entitled "Obama Order Sped Up Wave of Cyberattacks Against Iran" by David E. Sanger on Friday, June 1, 2012, and which information was provided and leaked to Mr. Sanger and the New York Times;
- 2) Any and all information that refers or relates in any way to information released to David E. Sanger and/or made available to him;

JA25



FREEDOM WATCH

▶ www.FreedomWatchUSA.org

▶ World Headquarters 2020 Pennsylvania Avenue, N.W., Suite 345, Washington, DC 20006-1811 ▶ (310) 595-0800 ▶ leklayman@gmail.com

Via Mail and Fax

June 1, 2012

OSD/JS FOIA Requester Service Center
Office of Freedom of Information
1155 Defense Pentagon
Washington, DC 20301-1155

Re: Freedom of Information Act Request

Dear Sir/Madam:

On June 1, 2012, the New York Times published two articles, "Obama Order Sped Up Wave of Cyberattacks Against Iran" by David E. Sanger. This article, a copy of which is attached, relied in large part on previously classified information which was released by Obama administration sources on the President's behalf. This released information is thus no longer classified and is no longer exempt from being released pursuant to the Freedom of Information Act. 5 U.S.C. 552 et seq.

Pursuant to the Freedom of Information Act (5 U.S.C. § 552 et seq.), Freedom Watch requests that that the Department of Defense produce all correspondence, memoranda, documents, reports, records, statements, audits, lists of names, applications, diskettes, letters, expense logs and receipts, calendar or diary logs, facsimile logs, telephone records call sheets, tape recordings, video/movie recordings, notes, examinations, opinions, folders, files, books, manuals, pamphlets, forms, drawings, charts, photographs, electronic mail, and other documents and things (hereinafter, "information") that refer or relate to the following in any way, within ten (10) business days as set forth below:

- 1) Any and all information that refers or relates to the New York Times article entitled "Obama Order Sped Up Wave of Cyberattacks Against Iran" by David E. Sanger on Friday, June 1, 2012, and which information was provided and leaked to Mr. Sanger and the New York Times;
- 2) Any and all information that refers or relates in any way to information released to David E. Sanger and/or made available to him;

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

FREEDOM WATCH, INC.,

Plaintiff,

v.

NATIONAL SECURITY AGENCY;
CENTRAL INTELLIGENCE AGENCY;
DEPARTMENT OF DEFENSE; and
DEPARTMENT OF STATE,

Defendants.

Case No. 1:12-cv-01088
Judge Robert L. Wilkins

EXHIBIT A

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

_____)	
FREEDOM WATCH, INC.)	
)	
Plaintiff,)	
)	
v.)	Civil Action No.: 1:12-cv-01088
)	
NATIONAL SECURITY AGENCY,)	
<i>et. al.</i>)	
)	
Defendants.)	
_____)	

DECLARATION OF PAMELA N. PHILLIPS

I, PAMELA N. PHILLIPS, hereby declare and state:

1. I am the current Chief of the Freedom of Information Act/Privacy Act (FOIA/PA) Office for the National Security Agency (hereinafter “NSA” or “the Agency”). I have served with NSA for thirty (30) years, and prior to my current assignment, I held various positions throughout the Agency. As the Chief, FOIA/PA Office, I am responsible for, among other things, the processing of all FOIA requests made directly to the Agency as well as FOIA requests directed to other agencies that involve records that originated with NSA and/or contain NSA equities. I am also responsible for asserting the FOIA exemptions over NSA on behalf of the Initial Denial Authority during the administrative processing of FOIA requests.

2. Through the exercise of my official duties, I have become familiar with the current litigation arising out of a FOIA request filed by Mr. Larry Klayman, attorney for the Plaintiff, Freedom Watch, Inc. The purpose of this declaration is to explain how the NSA

processed the Plaintiff's FOIA request and to inform the Court that the Plaintiff did not file an appeal of NSA's initial determinations, thereby failing to exhaust its administrative remedies.

PROCESSING OF PLAINTIFF'S FOIA REQUEST

3. By letter dated June 1, 2012, Plaintiff submitted a FOIA request to the NSA seeking records that refer or relate to an article from the New York Times entitled "Obama Order Sped Up Wave of Cyberattacks Against Iran" written by David E. Sanger and records that relate to information published in this article. Attachment 1. The Agency received Plaintiff's request on June 4, 2012.

4. My office processed Plaintiff's FOIA request and informed Plaintiff of its processing by letter dated June 11, 2012. Attachment 2. In this letter, my office informed Mr. Klayman that NSA did not assess any fees in processing his FOIA request and accordingly, it did not make a determination on his request for a fee waiver. Attachment 2, ¶ 1. Further, my office informed Mr. Klayman that NSA could not acknowledge the existence or nonexistence of the records he sought because such a response would reveal information that is currently and properly classified in accordance with Executive Order 13526 and thus exempt from release based on Exemption 1 of the FOIA.¹ Attachment 2, ¶ 2.

5. My office further informed Mr. Klayman in this letter that NSA could not acknowledge the existence or nonexistence of records responsive to his request because such a response is protected from release by cognizable Exemption 3 statutes,

¹ The refusal to confirm or deny the existence or nonexistence of records responsive to a FOIA request is commonly referred to as a *Glomar* response, under terminology derived from the D.C. Circuit's decision in *Phillipi v. CIA*, 546 F.2d 1009 (1976). There, the Central Intelligence Agency ("CIA") defended its refusal to confirm or deny the existence of records concerning the CIA's reported contacts with the media regarding a ship named *Hughes Glomar Explorer*. *Id.* at 1011.

specifically, Section 6 of the National Security Agency Act of 1959, 50 U.S.C. § 402 note (Pub. L. No. 86-36); and 50 U.S.C. § 403-1(i). Attachment 2, ¶ 3.

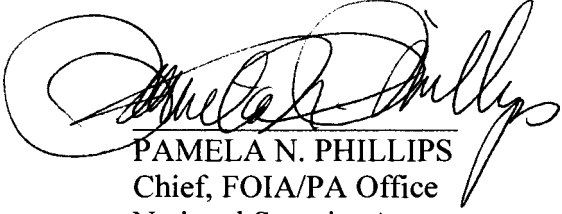
6. Finally, in this letter, my office informed Mr. Klayman of his right to appeal these determinations and explained to whom, how, where, and when to file such an appeal.

Attachment 2, ¶ 4.

7. Plaintiff did not appeal NSA's determinations as set forth in NSA's letter dated June 11, 2012. Rather, Plaintiff served NSA with a copy of a civil complaint, which was filed on June 28, 2012.

8. I declare under penalty of perjury that the facts set forth above are true and correct.

Executed, this 5th day of September 2012, pursuant to 28 U.S.C. §1746.


PAMELA N. PHILLIPS
Chief, FOIA/PA Office
National Security Agency

ATTACHMENT 1

DOCID: 3975419

REF ID: A3975419



FREEDOM WATCH

www.FreedomWatchUSA.org

World Headquarters 2020 Pennsylvania Avenue, N.W., Suite 145, Washington, DC 20006-1811 (310) 925-0800 info@freedomwatch.org

Via Mail and Fax

June 1, 2012

National Security Agency
Attn: FOIA/PA Office (DJP4)
9800 Savage Road, Suite 6248
Ft. George G. Meade, MD 20755-6248

Re: Freedom of Information Act Request

Dear Sir/Madam:

On June 1, 2012, the New York Times published two articles, "Obama Order Sped Up Wave of Cyberattacks Against Iran" by David E. Sanger. This article, a copy of which is attached, relied in large part on previously classified information which was released by Obama administration sources on the President's behalf. This released information is thus no longer classified and is no longer exempt from being released pursuant to the Freedom of Information Act, 5 U.S.C. 552 et seq.

Pursuant to the Freedom of Information Act (5 U.S.C. § 552 et seq.), Freedom Watch requests that that the National Security Agency produce all correspondence, memoranda, documents, reports, records, statements, audits, lists of names, applications, diskettes, letters, expense logs and receipts, calendar or diary logs, facsimile logs, telephone records call sheets, tape recordings, video/movie recordings, notes, examinations, opinions, folders, files, books, manuals, pamphlets, forms, drawings, charts, photographs, electronic mail, and other documents and things (hereinafter, "information") that refer or relate to the following in any way, within ten (10) business days as set forth below:

- 1) Any and all information that refers or relates to the New York Times article entitled "Obama Order Sped Up Wave of Cyberattacks Against Iran" by David E. Sanger on Friday, June 1, 2012, and which information was provided and leaked to Mr. Sanger and the New York Times;
- 2) Any and all information that refers or relates in any way to information released to David E. Sanger and/or made available to him;

JA32

DOCID: 3975419

National Security Agency
FOIA Request
Page | 2

- 3) The names of the persons, employers and job titles, and addresses of those who "leaked" the above information to David E. Sanger;
- 4) Communications with The White House and/or Office of the President and/or Vice President that refer or relate in any way to the "leaked" information and/or the reasons for "leaking" the information;
- 5) Any and all information that refer or relate to the decision to "leak" the above previously classified information;
- 6) Any and all information that refers or relates to government agencies deciding to investigate who "leaked" the above previously classified information.

If any responsive record or portion thereof is claimed to be exempt from production under FOIA, sufficient identifying information (with respect to each allegedly exempt record or portion thereof) must be provided to allow the assessment of the propriety of the claimed exemption. *Vaughn v. Rosen*, 484 F.2d 820 (D.C. Cir. 1973), *cert denied*, 415 U.S. 977 (1974). Additionally, pursuant to law, any reasonably segregable portion of a responsive record must be provided after redaction of any allegedly exempt material. 5 U.S.C. §552(b).

I request a waiver of all fees for this request under 5. U.S.C. § 552(a)(4)(A)(iii). Disclosure of the requested information to Freedom Watch is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in my commercial interest. The Islamic Republic of Iran's goal of obtaining nuclear weapons affects the safety of both Israel and the United States, thus putting American citizens at risk. Furthermore, the release of classified information by any particular individual within the executive branch, including the president, further endangers the American people and raises a spectre of corruption within the federal government that must be examined. Freedom Watch is engaged in the active dissemination of public information as is evident by our ongoing public interest legal work and continual fight against corruption within the United States government, and international cases, particularly with regard to Iran. Freedom Watch's website, freedomwatchusa.org serves as the primary means of disseminating that information, and is seen by millions of people annually. In addition, officials of Freedom Watch frequently appear on radio and television to disseminate important information to the public.

Furthermore, on behalf of Freedom Watch I am requesting expedited handling as provided in Department of Defense FOIA Regulation 54000.7-R because there is an urgency to inform the public about an actual or alleged federal government activity. Iran is reportedly on the verge of acquiring nuclear weapons and Israel is reportedly

DOCID: 3975419

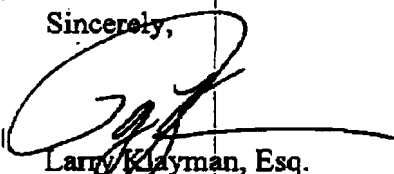
National Security Agency
FOIA Request
Page | 3

on the verge of attacking it to prevent their acquisition. The issue of a possible attack on Iran is of importance to the American people because Iran's acquiring of nuclear weapons places the safety of the American people as well as the safety of our allies in jeopardy. This war can break out any time because a strike is needed before Iran can gain the capability to build a bomb. This fact is also evidenced in the article mentioned above. There is an immediate clear and present danger to U.S. citizens, American military personnel.

The above mentioned "leaked" information is no longer in effect classified, if it ever was, as it was disclosed to the public by Mr. Sanger and The New York Times with the aid and complicity of President Obama and his administration. It was disclosed for political purposes to further President Obama's 2012 re-election campaign.

On behalf of Freedom Watch, I look forward to receiving the requested documents and a full fee waiver within ten (10) business days. You may have them delivered to the above address.

Sincerely,



Larry Klayman, Esq.
Chairman and General Counsel
2020 Pennsylvania Ave, N.W., Suite 345
Washington, D.C. 20006
leklayman@gmail.com

DOCID: 3975419 Obama Ordered Wave of Cyberattacks Against Iran - NYTimes.com REF ID: A3975419

The New York Times

June 1, 2012

Obama Order Sped Up Wave of Cyberattacks Against Iran

By DAVID E. SANGER

WASHINGTON — From his first months in office, President Obama secretly ordered increasingly sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, significantly expanding America's first sustained use of cyberweapons, according to participants in the program.

Mr. Obama decided to accelerate the attacks — begun in the Bush administration and code-named Olympic Games — even after an element of the program accidentally became public in the summer of 2010 because of a programming error that allowed it to escape Iran's Natanz plant and sent it around the world on the Internet. Computer security experts who began studying the worm, which had been developed by the United States and Israel, gave it a name: Stuxnet.

At a tense meeting in the White House Situation Room within days of the worm's "escape," Mr. Obama, Vice President Joseph R. Biden Jr. and the director of the Central Intelligence Agency at the time, Leon E. Panetta, considered whether America's most ambitious attempt to slow the progress of Iran's nuclear efforts had been fatally compromised.

"Should we shut this thing down?" Mr. Obama asked, according to members of the president's national security team who were in the room.

Told it was unclear how much the Iranians knew about the code, and offered evidence that it was still causing havoc, Mr. Obama decided that the cyberattacks should proceed. In the following weeks, the Natanz plant was hit by a newer version of the computer worm, and then another after that. The last of that series of attacks, a few weeks after Stuxnet was detected around the world, temporarily took out nearly 1,000 of the 5,000 centrifuges Iran had spinning at the time to purify uranium.

This account of the American and Israeli effort to undermine the Iranian nuclear program is based on interviews over the past 18 months with current and former American, European and Israeli officials involved in the program, as well as a range of outside experts. None would allow

DOCID: 3975419 Obama Ordered Wave of Cyberattacks Against Iran - NYTimes.com REF ID: A3975419

their names to be used because the effort remains highly classified, and parts of it continue to this day.

These officials gave differing assessments of how successful the sabotage program was in slowing Iran's progress toward developing the ability to build nuclear weapons. Internal Obama administration estimates say the effort was set back by 18 months to two years, but some experts inside and outside the government are more skeptical, noting that Iran's enrichment levels have steadily recovered, giving the country enough fuel today for five or more weapons, with additional enrichment.

Whether Iran is still trying to design and build a weapon is in dispute. The most recent United States intelligence estimate concludes that Iran suspended major parts of its weaponization effort after 2003, though there is evidence that some remnants of it continue.

Iran initially denied that its enrichment facilities had been hit by Stuxnet, then said it had found the worm and contained it. Last year, the nation announced that it had begun its own military cyberunit, and Brig. Gen. Gholamreza Jalali, the head of Iran's Passive Defense Organization, said that the Iranian military was prepared "to fight our enemies" in "cyberspace and Internet warfare." But there has been scant evidence that it has begun to strike back.

The United States government only recently acknowledged developing cyberweapons, and it has never admitted using them. There have been reports of one-time attacks against personal computers used by members of Al Qaeda, and of contemplated attacks against the computers that run air defense systems, including during the NATO-led air attack on Libya last year. But Olympic Games was of an entirely different type and sophistication.

It appears to be the first time the United States has repeatedly used cyberweapons to cripple another country's infrastructure, achieving, with computer code, what until then could be accomplished only by bombing a country or sending in agents to plant explosives. The code itself is 50 times as big as the typical computer worm, Carey Nachenberg, a vice president of Symantec, one of the many groups that have dissected the code, said at a symposium at Stanford University in April. Those forensic investigations into the inner workings of the code, while picking apart how it worked, came to no conclusions about who was responsible.

A similar process is now under way to figure out the origins of another cyberweapon called Flame that was recently discovered to have attacked the computers of Iranian officials, sweeping up information from those machines. But the computer code appears to be at least five years old, and American officials say that it was not part of Olympic Games. They have declined to say whether the United States was responsible for the Flame attack.

DOCID: 3975419 Obama Ordered Wave of Cyberattacks Against Iran - NYTimes.com ID: A0938449

Mr. Obama, according to participants in the many Situation Room meetings on Olympic Games, was acutely aware that with every attack he was pushing the United States into new territory, much as his predecessors had with the first use of atomic weapons in the 1940s, of intercontinental missiles in the 1950s and of drones in the past decade. He repeatedly expressed concerns that any American acknowledgment that it was using cyberweapons — even under the most careful and limited circumstances — could enable other countries, terrorists or hackers to justify their own attacks.

“We discussed the irony, more than once,” one of his aides said. Another said that the administration was resistant to developing a “grand theory for a weapon whose possibilities they were still discovering.” Yet Mr. Obama concluded that when it came to stopping Iran, the United States had no other choice.

If Olympic Games failed, he told aides, there would be no time for sanctions and diplomacy with Iran to work. Israel could carry out a conventional military attack, prompting a conflict that could spread throughout the region.

A Bush Initiative

The impetus for Olympic Games dates from 2006, when President George W. Bush saw few good options in dealing with Iran. At the time, America’s European allies were divided about the cost that imposing sanctions on Iran would have on their own economies. Having falsely accused Saddam Hussein of reconstituting his nuclear program in Iraq, Mr. Bush had little credibility in publicly discussing another nation’s nuclear ambitions. The Iranians seemed to sense his vulnerability, and, frustrated by negotiations, they resumed enriching uranium at an underground site at Natanz, one whose existence had been exposed just three years before.

Iran’s president, Mahmoud Ahmadinejad, took reporters on a tour of the plant and described grand ambitions to install upward of 50,000 centrifuges. For a country with only one nuclear power reactor — whose fuel comes from Russia — to say that it needed fuel for its civilian nuclear program seemed dubious to Bush administration officials. They feared that the fuel could be used in another way besides providing power: to create a stockpile that could later be enriched to bomb-grade material if the Iranians made a political decision to do so.

Hawks in the Bush administration like Vice President Dick Cheney urged Mr. Bush to consider a military strike against the Iranian nuclear facilities before they could produce fuel suitable for a weapon. Several times, the administration reviewed military options and concluded that they would only further inflame a region already at war, and would have uncertain results.

For years the C.I.A. had introduced faulty parts and designs into Iran’s systems — even

DOCID: 3975419 Obama Ordered Wave of Cyberattacks Against Iran - NYTimes.com REF ID: A3975419

tinkering with imported power supplies so that they would blow up — but the sabotage had had relatively little effect. General James E. Cartwright, who had established a small cyberoperation inside the United States Strategic Command, which is responsible for many of America's nuclear forces, joined intelligence officials in presenting a radical new idea to Mr. Bush and his national security team. It involved a far more sophisticated cyberweapon than the United States had designed before.

The goal was to gain access to the Natanz plant's industrial computer controls. That required leaping the electronic moat that cut the Natanz plant off from the Internet — called the air gap, because it physically separates the facility from the outside world. The computer code would invade the specialized computers that command the centrifuges.

The first stage in the effort was to develop a bit of computer code called a beacon that could be inserted into the computers, which were made by the German company Siemens and an Iranian manufacturer, to map their operations. The idea was to draw the equivalent of an electrical blueprint of the Natanz plant, to understand how the computers control the giant silvery centrifuges that spin at tremendous speeds. The connections were complex, and unless every circuit was understood, efforts to seize control of the centrifuges could fail.

Eventually the beacon would have to “phone home” — literally send a message back to the headquarters of the National Security Agency that would describe the structure and daily rhythms of the enrichment plant. Expectations for the plan were low; one participant said the goal was simply to “throw a little sand in the gears” and buy some time. Mr. Bush was skeptical, but lacking other options, he authorized the effort.

Breakthrough, Aided by Israel

It took months for the beacons to do their work and report home, complete with maps of the electronic directories of the controllers and what amounted to blueprints of how they were connected to the centrifuges deep underground.

Then the N.S.A. and a secret Israeli unit respected by American intelligence of cyberskills set to work developing the enormously complex computer worm that would separate the attacker from within.

The unusually tight collaboration with Israel was driven by two imperatives. In a part of its military, had technical expertise that rivaled the N.S.A.'s, and the Israelis had deep intelligence about operations at Natanz that would be vital to making the cyberattack a success. But American officials had another interest, to dissuade the Israelis from carrying out their own pre-emptive strike against the Iranian nuclear facilities. To do that, the Israelis would have to

4 MORE IN MI
OPEN Egypt A
Verdict
Read More

DOCID: 3975419 Obama Ordered Wave of Cyberattacks Against Iran - NYTimes.com REF ID: A3975419

be convinced that the new line of attack was working. The only way to convince them, several officials said in interviews, was to have them deeply involved in every aspect of the program.

Soon the two countries had developed a complex worm that the Americans called "the bug." But the bug needed to be tested. So, under enormous secrecy, the United States began building replicas of Iran's P-1 centrifuges, an aging, unreliable design that Iran purchased from Abdul Qadeer Khan, the Pakistani nuclear chief who had begun selling fuel-making technology on the black market. Fortunately for the United States, it already owned some P-1s, thanks to the Libyan dictator, Col. Muammar el-Qaddafi.

When Colonel Qaddafi gave up his nuclear weapons program in 2003, he turned over the centrifuges he had bought from the Pakistani nuclear ring, and they were placed in storage at a weapons laboratory in Tennessee. The military and intelligence officials overseeing Olympic Games borrowed some for what they termed "destructive testing," essentially building a virtual replica of Natanz, but spreading the test over several of the Energy Department's national laboratories to keep even the most trusted nuclear workers from figuring out what was afoot.

Those first small-scale tests were surprisingly successful: the bug invaded the computers, lurking for days or weeks, before sending instructions to speed them up or slow them down so suddenly that their delicate parts, spinning at supersonic speeds, self-destructed. After several false starts, it worked. One day, toward the end of Mr. Bush's term, the rubble of a centrifuge was spread out on the conference table in the Situation Room, proof of the potential power of a cyberweapon. The worm was declared ready to test against the real target: Iran's underground enrichment plant.

"Previous cyberattacks had effects limited to other computers," Michael V. Hayden, the former chief of the C.I.A., said, declining to describe what he knew of these attacks when he was in office. "This is the first attack of a major nature in which a cyberattack was used to effect physical destruction," rather than just slow another computer, or hack into it to steal data.

"Somebody crossed the Rubicon," he said.

Getting the worm into Natanz, however, was no easy trick. The United States and Israel would have to rely on engineers, maintenance workers and others — both spies and unwitting accomplices — with physical access to the plant. "That was our holy grail," one of the architects of the plan said. "It turns out there is always an idiot around who doesn't think much about the thumb drive in their hand."

In fact, thumb drives turned out to be critical in spreading the first variants of the computer worm; later, more sophisticated methods were developed to deliver the malicious code.

DOCID: 3975419 Obama Ordered Wave of Cyberattacks Against Iran - NYTimes.com REF ID: A3975419

The first attacks were small, and when the centrifuges began spinning out of control in 2008, the Iranians were mystified about the cause, according to intercepts that the United States later picked up. "The thinking was that the Iranians would blame bad parts, or bad engineering, or just incompetence," one of the architects of the early attack said.

The Iranians were confused partly because no two attacks were exactly alike. Moreover, the code would lurk inside the plant for weeks, recording normal operations; when it attacked, it sent signals to the Natanz control room indicating that everything downstairs was operating normally. "This may have been the most brilliant part of the code," one American official said.

Later, word circulated through the International Atomic Energy Agency, the Vienna-based nuclear watchdog, that the Iranians had grown so distrustful of their own instruments that they had assigned people to sit in the plant and radio back what they saw.

"The intent was that the failures should make them feel they were stupid, which is what happened," the participant in the attacks said. When a few centrifuges failed, the Iranians would close down whole "stands" that linked 164 machines, looking for signs of sabotage in all of them. "They overreacted," one official said. "We soon discovered they fired people."

Imagery recovered by nuclear inspectors from cameras at Natanz — which the nuclear agency uses to keep track of what happens between visits — showed the results: There was some evidence of wreckage, but it was clear that the Iranians had also carted away centrifuges that had previously appeared to be working well.

But by the time Mr. Bush left office, no wholesale destruction had been accomplished. Meeting with Mr. Obama in the White House days before his inauguration, Mr. Bush urged him to preserve two classified programs, Olympic Games and the drone program in Pakistan. Mr. Obama took Mr. Bush's advice.

The Stuxnet Surprise

Mr. Obama came to office with an interest in cyberissues, but he had discussed them during the campaign mostly in terms of threats to personal privacy and the risks to infrastructure like the electrical grid and the air traffic control system. He commissioned a major study on how to improve America's defenses and announced it with great fanfare in the East Room.

What he did not say then was that he was also learning the arts of cyberwar. The architects of Olympic Games would meet him in the Situation Room, often with what they called the "horse blanket," a giant foldout schematic diagram of Iran's nuclear production facilities. Mr. Obama authorized the attacks to continue, and every few weeks — certainly after a major attack — he

DOCID: 3975419 Obama Ordered Wave of Cyberattacks Against Iran - NYTimes.com ID: 3975419

would get updates and authorize the next step. Sometimes it was a strike riskier and bolder than what had been tried previously.

"From his first days in office, he was deep into every step in slowing the Iranian program — the diplomacy, the sanctions, every major decision," a senior administration official said. "And it's safe to say that whatever other activity might have been under way was no exception to that rule."

But the good luck did not last. In the summer of 2010, shortly after a new variant of the worm had been sent into Natanz, it became clear that the worm, which was never supposed to leave the Natanz machines, had broken free, like a zoo animal that found the keys to the cage. It fell to Mr. Panetta and two other crucial players in Olympic Games — General Cartwright, the vice chairman of the Joint Chiefs of Staff, and Michael J. Morell, the deputy director of the CIA — to break the news to Mr. Obama and Mr. Biden.

An error in the code, they said, had led it to spread to an engineer's computer when it was hooked up to the centrifuges. When the engineer left Natanz and connected the computer to the Internet, the American- and Israeli-made bug failed to recognize that its environment had changed. It began replicating itself all around the world. Suddenly, the code was exposed, though its intent would not be clear, at least to ordinary computer users.

"We think there was a modification done by the Israelis," one of the briefers told the president, "and we don't know if we were part of that activity."

Mr. Obama, according to officials in the room, asked a series of questions, fearful that the code could do damage outside the plant. The answers came back in hedged terms. Mr. Biden fumed. "It's got to be the Israelis," he said. "They went too far."

In fact, both the Israelis and the Americans had been aiming for a particular part of the centrifuge plant, a critical area whose loss, they had concluded, would set the Iranians back considerably. It is unclear who introduced the programming error.

The question facing Mr. Obama was whether the rest of Olympic Games was in jeopardy, now that a variant of the bug was replicating itself "in the wild," where computer security experts can dissect it and figure out its purpose.

"I don't think we have enough information," Mr. Obama told the group that day, according to the officials. But in the meantime, he ordered that the cyberattacks continue. They were his best hope of disrupting the Iranian nuclear program unless economic sanctions began to bite harder and reduced Iran's oil revenues.

DOCID: 3975419 Obama Ordered Wave of Cyberattacks Against Iran - NYTimes.com REF ID: A3975419

Within a week, another version of the bug brought down just under 1,000 centrifuges. Olympic Games was still on.

A Weapon's Uncertain Future

American cyberattacks are not limited to Iran, but the focus of attention, as one administration official put it, "has been overwhelmingly on one country." There is no reason to believe that will remain the case for long. Some officials question why the same techniques have not been used more aggressively against North Korea. Others see chances to disrupt Chinese military plans, forces in Syria on the way to suppress the uprising there, and Qaeda operations around the world. "We've considered a lot more attacks than we have gone ahead with," one former intelligence official said.

Mr. Obama has repeatedly told his aides that there are risks to using — and particularly to overusing — the weapon. In fact, no country's infrastructure is more dependent on computer systems, and thus more vulnerable to attack, than that of the United States. It is only a matter of time, most experts believe, before it becomes the target of the same kind of weapon that the Americans have used, secretly, against Iran.

This article is adapted from "Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power," to be published by Crown on Tuesday.

DOCID: 3975419

REF ID: A3975419



FREEDOM WATCH

www.FreedomWatchUSA.org

World Headquarters 2820 Pennsylvania Avenue, N.W., Suite 345, Washington, DC 20006-1811 (310) 595-0800 info@freedomwatch.org

FAX

To: National Security Agency **From:** Freedom Watch

Fax: 443-479-3612 **Pages:** 11 (excluding this one)

Phone: **Date:** 06-01-12

Re: FOIA Request **CC:**

- Urgent For Review Please Comment Please Reply

ATTACHMENT 2



NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 67855
11 June 2012

Larry E. Klayman, Esquire
2020 Pennsylvania Ave., NW, Suite 345
Washington, DC 20006

Dear Mr. Klayman:

This responds to your Freedom of Information Act (FOIA) request of 1 June 2012, which was received by this office on 4 June 2012, for the following:

1. "Any and all information that refers or relates to the New York Times article entitled 'Obama Order Sped Up Wave of Cyberattacks Against Iran' by David E. Sanger on Friday, June 1, 2012, and which information was provided and leaked to Mr. Sanger and the New York Times;
2. Any and all information that refers or relates in any way to information released to David E. Sanger and/or made available to him;
3. The names of the persons, employees, and job titles and addresses of those who 'leaked' the above information to David E. Sanger;
4. Communications with The White House and/or Office of the President and/or Vice President that refer or relate in any way to the 'leaked' information and/or reasons for 'leaking' the information;
5. Any and all information that refer or relate to the decision to 'leak' the above previously classified information;
6. Any and all information that refers or relates to government agencies deciding to investigate who 'leaked' the above previously classified information."

Your letter has been assigned Case Number 67855. Please refer to this case number when contacting us about your request. For purposes of this request and based on the information you provided in your letter, you are considered an "all other" requester. There are no assessable fees for this request; therefore, we did not address your request for a fee waiver. Your request has been processed under the provisions of the FOIA.

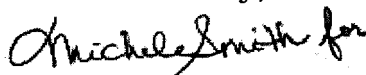
FOIA Case: 67855

We have determined that the fact of the existence or non-existence of the materials you request is a currently and properly classified matter in accordance with Executive Order 13526, as set forth in Subparagraph (c) of Section 1.4. Thus, your request is denied pursuant to the first exemption of the FOIA which provides that the FOIA does not apply to matters that are specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign relations and are, in fact properly classified pursuant to such Executive Order.

In addition, this Agency is authorized by various statutes to protect certain information concerning its activities. The third exemption of the FOIA provides for the withholding of information specifically protected from disclosure by statute. Thus, your request is also denied because the fact of the existence or non-existence of the information is exempted from disclosure pursuant to the third exemption. The specific statutes applicable in this case are Title 50 U.S. Code 403-1(i); and Section 6, Public Law 86-36 (50 U.S. Code 402 note).

The Initial Denial Authority for NSA information is the Deputy Associate Director for Policy and Records, D. M. Janosek. As your request is being denied, you are hereby advised of this Agency's appeal procedures. Any person denied access to information may file an appeal to the NSA/CSS Freedom of Information Act Appeal Authority. The appeal must be postmarked no later than 60 calendar days of the date of the initial denial letter. The appeal shall be in writing addressed to the NSA/CSS FOIA Appeal Authority (DJ4), National Security Agency, 9800 Savage Road STE 6248, Fort George G. Meade, MD 20755-6248. The appeal shall reference the adverse determination and shall contain, in sufficient detail and particularity, the grounds upon which the requester believes that the determination is unwarranted. The NSA/CSS FOIA Appeal Authority will endeavor to respond to the appeal within 20 working days after receipt, absent any unusual circumstances.

Sincerely,



PAMELA N. PHILLIPS

Chief

FOIA/PA Office

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

FREEDOM WATCH, INC.,

Plaintiff,

v.

NATIONAL SECURITY AGENCY;
CENTRAL INTELLIGENCE AGENCY;
DEPARTMENT OF DEFENSE; and
DEPARTMENT OF STATE,

Defendants.

Case No. 1:12-cv-01088
Judge Robert L. Wilkins

EXHIBIT B

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

<u>FREEDOM WATCH, INC.,</u>)	
)	
<i>Plaintiff,</i>)	
)	
)	Civil Action No. 12-cv-1088-RLW
v.)	Judge Robert L. Wilkins
)	
NATIONAL SECURITY AGENCY,)	
<i>et al.</i>)	
)	
<u><i>Defendants.</i></u>)	

**DECLARATION OF MICHELE L. MEEKS
CHIEF, INFORMATION REVIEW AND RELEASE GROUP,
CENTRAL INTELLIGENCE AGENCY**

I, MICHELE L. MEEKS, hereby declare and state:

1. I am the Chief, Public Information Programs Division ("PIPD") in the Office of the Chief Information Officer, Central Intelligence Agency ("CIA"). I was assigned to this position in April, 2012, and simultaneously was appointed as the CIA Information and Privacy Coordinator ("IPC"). Prior to these dual assignments, I served as the Acting Chief, PIPD, from February to April 2012, and the Deputy Chief, PIPD, from July 2011 to April 2012.

2. In my capacities as Chief of PIPD and the IPC, I am responsible for managing the Freedom of Information Act ("FOIA"), Privacy Act ("PA"), and Executive Order 13,526 (E.O. 13,526) Mandatory Declassification Review ("MDR") programs in

the CIA. These responsibilities include directing searches of CIA records systems pursuant to public requests for records under these programs, and coordinating the reviews of any records retrieved in such searches. As part of my official duties, I ensure that the Agency administratively processes records requests, including the search, retrieval, analysis, review, redaction, and release of documents, in accordance with the law and as efficiently as possible with the personnel and resources available.

3. As the IPC, I also possess original classification authority at the TOP SECRET level under a written delegation of authority in accordance with E.O. 13,526. See Exec. Order No. 13,526, § 1.3(c), 75 Fed. Reg. 707, 708 (Jan. 5, 2010). This means that I am authorized to assess the current, proper classification of CIA information, up to and including TOP SECRET information, based on the classification criteria of E.O. 13,526 and applicable regulations.

4. Through the exercise of my official duties, I have become familiar with this civil action and Plaintiff's underlying requests for information. I make the following statements based upon my personal knowledge and information made available to me in my official capacity.

5. By way of letter, dated 1 June 2012, Mr. Klayman requested information from the CIA under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552. The letter is attached hereto as Exhibit 1. In his request, Mr. Klayman sought information related to a New York Times article titled "Obama Order Sped Up Wave of Cyberattacks Against Iran." Mr. Klayman also requested expedited processing and a waiver of all fees.

6. On 12 June 2012, the CIA responded to Mr. Klayman by letter, attached hereto as Exhibit 2. The letter assigned tracking number F-2012-01429 to Mr. Klayman's request, but informed him that the Agency could neither confirm nor deny the existence of records responsive to his request.¹ The letter further stated that the existence or nonexistence of such records was classified, and related to intelligence sources and methods, and was therefore being withheld on the basis of FOIA exemptions (b) (1) and (b) (3). The letter did not address Mr. Klayman's request for a fee waiver. Given the Agency's Glomar determination, Mr. Klayman's request incurred no charges.

7. Finally, the letter informed Mr. Klayman of his right to appeal the CIA's decision to the Agency Review Panel within 45 days of the date of the letter. Mr. Klayman has never appealed

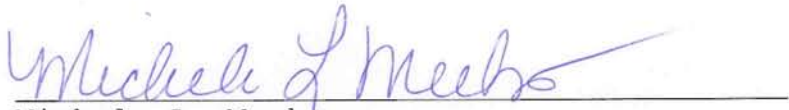
¹ A government agency's refusal to confirm or deny the existence or nonexistence of records responsive to a FOIA request is commonly referred to as a "Glomar response" after Phillippi v. CIA, 546 F.2d 1009 (D.C. Cir. 1976).

the CIA's determination, and the time to appeal has passed. Instead, I understand that Mr. Klayman filed suit on 28 June 2012. The CIA has received no other correspondence from Mr. Klayman related to this request.

* * *

I declare, under penalty of perjury, that the foregoing is true and correct.

Executed this 4th day of October, 2012.


Michele L. Meeks
Chief, Public Information Programs
Division and Information & Privacy
Coordinator,
Central Intelligence Agency

ATTACHMENT 1

F-2012-01429



FREEDOM WATCH

www.FreedomWatchUSA.org

World Headquarters 2020 Pennsylvania Avenue, N.W., Suite 345, Washington, DC 20006-1811 (310) 595-0800 info@freedomwatch.org

Via Mail and Fax

June 1, 2012

Information and Privacy Coordinator
Central Intelligence Agency
Washington, D.C. 20505

Re: Freedom of Information Act Request

Dear Sir/Madam:

On June 1, 2012, the New York Times published two articles, "Obama Order Sped Up Wave of Cyberattacks Against Iran" by David E. Sanger. This article, a copy of which is attached, relied in large part on previously classified information which was released by Obama administration sources on the President's behalf. This released information is thus no longer classified and is no longer exempt from being released pursuant to the Freedom of Information Act. 5 U.S.C. 552 et seq.

Pursuant to the Freedom of Information Act (5 U.S.C. § 552 et seq.), Freedom Watch requests that that the Central Intelligence Agency produce all correspondence, memoranda, documents, reports, records, statements, audits, lists of names, applications, diskettes, letters, expense logs and receipts, calendar or diary logs, facsimile logs, telephone records call sheets, tape recordings, video/movie recordings, notes, examinations, opinions, folders, files, books, manuals, pamphlets, forms, drawings, charts, photographs, electronic mail, and other documents and things (hereinafter, "information") that refer or relate to the following in any way, within ten (10) business days as set forth below:

- 1) Any and all information that refers or relates to the New York Times article entitled "Obama Order Sped Up Wave of Cyberattacks Against Iran" by David E. Sanger on Friday, June 1, 2012, and which information was provided and leaked to Mr. Sanger and the New York Times;
- 2) Any and all information that refers or relates in any way to information released to David E. Sanger and/or made available to him;

JUN - 1 2012

Central Intelligence Agency
FOIA Request
Page | 2

- 3) The names of the persons, employers and job titles, and addresses of those who "leaked" the above information to David E. Sanger
- 4) Communications with The White House and/or Office of the President and/or Vice President that refer or relate in any way to the "leaked" information and/or the reasons for "leaking" the information;
- 5) Any and all information that refer or relate to the decision to "leak" the above previously classified information;
- 6) Any and all information that refers or relates to government agencies deciding to investigate who "leaked" the above previously classified information.

If any responsive record or portion thereof is claimed to be exempt from production under FOIA, sufficient identifying information (with respect to each allegedly exempt record or portion thereof) must be provided to allow the assessment of the propriety of the claimed exemption. *Vaughn v. Rosen*, 484 F.2d 820 (D.C. Cir. 1973), *cert denied*, 415 U.S. 977 (1974). Additionally, pursuant to law, any reasonably segregable portion of a responsive record must be provided after redaction of any allegedly exempt material. 5 U.S.C. §552(b).

I request a waiver of all fees for this request under 5. U.S.C. § 552(a)(4)(A)(iii). Disclosure of the requested information to Freedom Watch is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in my commercial interest. The Islamic Republic of Iran's goal of obtaining nuclear weapons affects the safety of both Israel and the United States, thus putting American citizens at risk. Furthermore, the release of classified information by any particular individual within the executive branch, including the president, further endangers the American people and raises a spectre of corruption within the federal government that must be examined. Freedom Watch is engaged in the active dissemination of public information as is evident by our ongoing public interest legal work and continual fight against corruption within the United States government, and international cases, particularly with regard to Iran. Freedom Watch's website, freedomwatchusa.org serves as the primary means of disseminating that information, and is seen by millions of people annually. In addition, officials of Freedom Watch frequently appear on radio and television to disseminate important information to the public.

Furthermore, on behalf of Freedom Watch I am requesting expedited handling as provided in 32 C.F.R. 1900.3 because there is an urgency to inform the public about an actual or alleged federal government activity. Iran is reportedly on the verge of acquiring nuclear weapons and Israel is reportedly on the verge of attacking it to

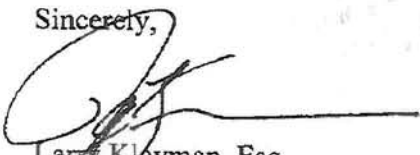
Central Intelligence Agency
FOIA Request
Page | 3

prevent their acquisition. The issue of a possible attack on Iran is of importance to the American people because Iran's acquiring of nuclear weapons places the safety of the American people as well as the safety of our allies in jeopardy. This war can break out any time because a strike is needed before Iran can gain the capability to build a bomb. This fact is also evidenced in the article mentioned above. There is an immediate clear and present danger to U.S. citizens, American military personnel.

The above mentioned "leaked" information is no longer in effect classified, if it ever was, as it was disclosed to the public by Mr. Sanger and The New York Times with the aid and complicity of President Obama and his administration. It was disclosed for political purposes to further President Obama's 2012 re-election campaign.

On behalf of Freedom Watch, I look forward to receiving the requested documents and a full fee waiver within ten (10) business days. You may have them delivered to the above address.

Sincerely,



Larry Klayman, Esq.
Chairman and General Counsel
2020 Pennsylvania Ave, N.W., Suite 345
Washington, D.C. 20006
leklayman@gmail.com

6/1/12

Obama Ordered Wave of Cyberattacks Against Iran - NYTimes.com

The New York Times

June 1, 2012

Obama Order Sped Up Wave of Cyberattacks Against Iran

By DAVID E. SANGER

WASHINGTON — From his first months in office, President Obama secretly ordered increasingly sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, significantly expanding America's first sustained use of cyberweapons, according to participants in the program.

Mr. Obama decided to accelerate the attacks — begun in the Bush administration and code-named Olympic Games — even after an element of the program accidentally became public in the summer of 2010 because of a programming error that allowed it to escape Iran's Natanz plant and sent it around the world on the Internet. Computer security experts who began studying the worm, which had been developed by the United States and Israel, gave it a name: Stuxnet.

At a tense meeting in the White House Situation Room within days of the worm's "escape," Mr. Obama, Vice President Joseph R. Biden Jr. and the director of the Central Intelligence Agency at the time, Leon E. Panetta, considered whether America's most ambitious attempt to slow the progress of Iran's nuclear efforts had been fatally compromised.

"Should we shut this thing down?" Mr. Obama asked, according to members of the president's national security team who were in the room.

Told it was unclear how much the Iranians knew about the code, and offered evidence that it was still causing havoc, Mr. Obama decided that the cyberattacks should proceed. In the following weeks, the Natanz plant was hit by a newer version of the computer worm, and then another after that. The last of that series of attacks, a few weeks after Stuxnet was detected around the world, temporarily took out nearly 1,000 of the 5,000 centrifuges Iran had spinning at the time to purify uranium.

This account of the American and Israeli effort to undermine the Iranian nuclear program is based on interviews over the past 18 months with current and former American, European and Israeli officials involved in the program, as well as a range of outside experts. None would allow

6/1/12

Obama Ordered Wave of Cyberattacks Against Iran - NYTimes.com

their names to be used because the effort remains highly classified, and parts of it continue to this day.

These officials gave differing assessments of how successful the sabotage program was in slowing Iran's progress toward developing the ability to build nuclear weapons. Internal Obama administration estimates say the effort was set back by 18 months to two years, but some experts inside and outside the government are more skeptical, noting that Iran's enrichment levels have steadily recovered, giving the country enough fuel today for five or more weapons, with additional enrichment.

Whether Iran is still trying to design and build a weapon is in dispute. The most recent United States intelligence estimate concludes that Iran suspended major parts of its weaponization effort after 2003, though there is evidence that some remnants of it continue.

Iran initially denied that its enrichment facilities had been hit by Stuxnet, then said it had found the worm and contained it. Last year, the nation announced that it had begun its own military cyberunit, and Brig. Gen. Gholamreza Jalali, the head of Iran's Passive Defense Organization, said that the Iranian military was prepared "to fight our enemies" in "cyberspace and Internet warfare." But there has been scant evidence that it has begun to strike back.

The United States government only recently acknowledged developing cyberweapons, and it has never admitted using them. There have been reports of one-time attacks against personal computers used by members of Al Qaeda, and of contemplated attacks against the computers that run air defense systems, including during the NATO-led air attack on Libya last year. But Olympic Games was of an entirely different type and sophistication.

It appears to be the first time the United States has repeatedly used cyberweapons to cripple another country's infrastructure, achieving, with computer code, what until then could be accomplished only by bombing a country or sending in agents to plant explosives. The code itself is 50 times as big as the typical computer worm, Carey Nachenberg, a vice president of Symantec, one of the many groups that have dissected the code, said at a symposium at Stanford University in April. Those forensic investigations into the inner workings of the code, while picking apart how it worked, came to no conclusions about who was responsible.

A similar process is now under way to figure out the origins of another cyberweapon called Flame that was recently discovered to have attacked the computers of Iranian officials, sweeping up information from those machines. But the computer code appears to be at least five years old, and American officials say that it was not part of Olympic Games. They have declined to say whether the United States was responsible for the Flame attack.

6/1/12

Obama Ordered Wave of Cyberattacks Against Iran - NYTimes.com

Mr. Obama, according to participants in the many Situation Room meetings on Olympic Games, was acutely aware that with every attack he was pushing the United States into new territory, much as his predecessors had with the first use of atomic weapons in the 1940s, of intercontinental missiles in the 1950s and of drones in the past decade. He repeatedly expressed concerns that any American acknowledgment that it was using cyberweapons — even under the most careful and limited circumstances — could enable other countries, terrorists or hackers to justify their own attacks.

“We discussed the irony, more than once,” one of his aides said. Another said that the administration was resistant to developing a “grand theory for a weapon whose possibilities they were still discovering.” Yet Mr. Obama concluded that when it came to stopping Iran, the United States had no other choice.

If Olympic Games failed, he told aides, there would be no time for sanctions and diplomacy with Iran to work. Israel could carry out a conventional military attack, prompting a conflict that could spread throughout the region.

A Bush Initiative

The impetus for Olympic Games dates from 2006, when President George W. Bush saw few good options in dealing with Iran. At the time, America’s European allies were divided about the cost that imposing sanctions on Iran would have on their own economies. Having falsely accused Saddam Hussein of reconstituting his nuclear program in Iraq, Mr. Bush had little credibility in publicly discussing another nation’s nuclear ambitions. The Iranians seemed to sense his vulnerability, and, frustrated by negotiations, they resumed enriching uranium at an underground site at Natanz, one whose existence had been exposed just three years before.

Iran’s president, Mahmoud Ahmadinejad, took reporters on a tour of the plant and described grand ambitions to install upward of 50,000 centrifuges. For a country with only one nuclear power reactor — whose fuel comes from Russia — to say that it needed fuel for its civilian nuclear program seemed dubious to Bush administration officials. They feared that the fuel could be used in another way besides providing power: to create a stockpile that could later be enriched to bomb-grade material if the Iranians made a political decision to do so.

Hawks in the Bush administration like Vice President Dick Cheney urged Mr. Bush to consider a military strike against the Iranian nuclear facilities before they could produce fuel suitable for a weapon. Several times, the administration reviewed military options and concluded that they would only further inflame a region already at war, and would have uncertain results.

For years the C.I.A. had introduced faulty parts and designs into Iran’s systems — even

tinkering with imported power supplies so that they would blow up — but the sabotage had had relatively little effect. General James E. Cartwright, who had established a small cyberoperation inside the United States Strategic Command, which is responsible for many of America’s nuclear forces, joined intelligence officials in presenting a radical new idea to Mr. Bush and his national security team. It involved a far more sophisticated cyberweapon than the United States had designed before.

The goal was to gain access to the Natanz plant’s industrial computer controls. That required leaping the electronic moat that cut the Natanz plant off from the Internet — called the air gap, because it physically separates the facility from the outside world. The computer code would invade the specialized computers that command the centrifuges.

The first stage in the effort was to develop a bit of computer code called a beacon that could be inserted into the computers, which were made by the German company Siemens and an Iranian manufacturer, to map their operations. The idea was to draw the equivalent of an electrical blueprint of the Natanz plant, to understand how the computers control the giant silvery centrifuges that spin at tremendous speeds. The connections were complex, and unless every circuit was understood, efforts to seize control of the centrifuges could fail.

Eventually the beacon would have to “phone home” — literally send a message back to the headquarters of the National Security Agency that would describe the structure and daily rhythms of the enrichment plant. Expectations for the plan were low; one participant said the goal was simply to “throw a little sand in the gears” and buy some time. Mr. Bush was skeptical, but lacking other options, he authorized the effort.

Breakthrough, Aided by Israel

It took months for the beacons to do their work and report home, complete with maps of the electronic directories of the controllers and what amounted to blueprints of how they were connected to the centrifuges deep underground.

Then the N.S.A. and a secret Israeli unit respected by American intelligence of cyberskills set to work developing the enormously complex computer worm that the attacker from within.

◀ OPEN MORE IN MI
Egypt A Verdict
Read More

The unusually tight collaboration with Israel was driven by two imperatives. I a part of its military, had technical expertise that rivaled the N.S.A.’s, and the Israelis had deep intelligence about operations at Natanz that would be vital to making the cyberattack a success. But American officials had another interest, to dissuade the Israelis from carrying out their own pre-emptive strike against the Iranian nuclear facilities. To do that, the Israelis would have to

6/1/12

Obama Ordered Wave of Cyberattacks Against Iran - NYTimes.com

be convinced that the new line of attack was working. The only way to convince them, several officials said in interviews, was to have them deeply involved in every aspect of the program.

Soon the two countries had developed a complex worm that the Americans called "the bug." But the bug needed to be tested. So, under enormous secrecy, the United States began building replicas of Iran's P-1 centrifuges, an aging, unreliable design that Iran purchased from Abdul Qadeer Khan, the Pakistani nuclear chief who had begun selling fuel-making technology on the black market. Fortunately for the United States, it already owned some P-1s, thanks to the Libyan dictator, Col. Muammar el-Qaddafi.

When Colonel Qaddafi gave up his nuclear weapons program in 2003, he turned over the centrifuges he had bought from the Pakistani nuclear ring, and they were placed in storage at a weapons laboratory in Tennessee. The military and intelligence officials overseeing Olympic Games borrowed some for what they termed "destructive testing," essentially building a virtual replica of Natanz, but spreading the test over several of the Energy Department's national laboratories to keep even the most trusted nuclear workers from figuring out what was afoot.

Those first small-scale tests were surprisingly successful: the bug invaded the computers, lurking for days or weeks, before sending instructions to speed them up or slow them down so suddenly that their delicate parts, spinning at supersonic speeds, self-destructed. After several false starts, it worked. One day, toward the end of Mr. Bush's term, the rubble of a centrifuge was spread out on the conference table in the Situation Room, proof of the potential power of a cyberweapon. The worm was declared ready to test against the real target: Iran's underground enrichment plant.

"Previous cyberattacks had effects limited to other computers," Michael V. Hayden, the former chief of the C.I.A., said, declining to describe what he knew of these attacks when he was in office. "This is the first attack of a major nature in which a cyberattack was used to effect physical destruction," rather than just slow another computer, or hack into it to steal data.

"Somebody crossed the Rubicon," he said.

Getting the worm into Natanz, however, was no easy trick. The United States and Israel would have to rely on engineers, maintenance workers and others — both spies and unwitting accomplices — with physical access to the plant. "That was our holy grail," one of the architects of the plan said. "It turns out there is always an idiot around who doesn't think much about the thumb drive in their hand."

In fact, thumb drives turned out to be critical in spreading the first variants of the computer worm; later, more sophisticated methods were developed to deliver the malicious code.

6/1/12

Obama Ordered Wave of Cyberattacks Against Iran - NYTimes.com

The first attacks were small, and when the centrifuges began spinning out of control in 2008, the Iranians were mystified about the cause, according to intercepts that the United States later picked up. "The thinking was that the Iranians would blame bad parts, or bad engineering, or just incompetence," one of the architects of the early attack said.

The Iranians were confused partly because no two attacks were exactly alike. Moreover, the code would lurk inside the plant for weeks, recording normal operations; when it attacked, it sent signals to the Natanz control room indicating that everything downstairs was operating normally. "This may have been the most brilliant part of the code," one American official said.

Later, word circulated through the International Atomic Energy Agency, the Vienna-based nuclear watchdog, that the Iranians had grown so distrustful of their own instruments that they had assigned people to sit in the plant and radio back what they saw.

"The intent was that the failures should make them feel they were stupid, which is what happened," the participant in the attacks said. When a few centrifuges failed, the Iranians would close down whole "stands" that linked 164 machines, looking for signs of sabotage in all of them. "They overreacted," one official said. "We soon discovered they fired people."

Imagery recovered by nuclear inspectors from cameras at Natanz — which the nuclear agency uses to keep track of what happens between visits — showed the results. There was some evidence of wreckage, but it was clear that the Iranians had also carted away centrifuges that had previously appeared to be working well.

But by the time Mr. Bush left office, no wholesale destruction had been accomplished. Meeting with Mr. Obama in the White House days before his inauguration, Mr. Bush urged him to preserve two classified programs, Olympic Games and the drone program in Pakistan. Mr. Obama took Mr. Bush's advice.

The Stuxnet Surprise

Mr. Obama came to office with an interest in cyberissues, but he had discussed them during the campaign mostly in terms of threats to personal privacy and the risks to infrastructure like the electrical grid and the air traffic control system. He commissioned a major study on how to improve America's defenses and announced it with great fanfare in the East Room.

What he did not say then was that he was also learning the arts of cyberwar. The architects of Olympic Games would meet him in the Situation Room, often with what they called the "horse blanket," a giant foldout schematic diagram of Iran's nuclear production facilities. Mr. Obama authorized the attacks to continue, and every few weeks — certainly after a major attack — he

6/1/12

Obama Ordered Wave of Cyberattacks Against Iran - NYTimes.com

would get updates and authorize the next step. Sometimes it was a strike riskier and bolder than what had been tried previously.

“From his first days in office, he was deep into every step in slowing the Iranian program — the diplomacy, the sanctions, every major decision,” a senior administration official said. “And it’s safe to say that whatever other activity might have been under way was no exception to that rule.”

But the good luck did not last. In the summer of 2010, shortly after a new variant of the worm had been sent into Natanz, it became clear that the worm, which was never supposed to leave the Natanz machines, had broken free, like a zoo animal that found the keys to the cage. It fell to Mr. Panetta and two other crucial players in Olympic Games — General Cartwright, the vice chairman of the Joint Chiefs of Staff, and Michael J. Morell, the deputy director of the C.I.A. — to break the news to Mr. Obama and Mr. Biden.

An error in the code, they said, had led it to spread to an engineer’s computer when it was hooked up to the centrifuges. When the engineer left Natanz and connected the computer to the Internet, the American- and Israeli-made bug failed to recognize that its environment had changed. It began replicating itself all around the world. Suddenly, the code was exposed, though its intent would not be clear, at least to ordinary computer users.

“We think there was a modification done by the Israelis,” one of the briefers told the president, “and we don’t know if we were part of that activity.”

Mr. Obama, according to officials in the room, asked a series of questions, fearful that the code could do damage outside the plant. The answers came back in hedged terms. Mr. Biden fumed. “It’s got to be the Israelis,” he said. “They went too far.”

In fact, both the Israelis and the Americans had been aiming for a particular part of the centrifuge plant, a critical area whose loss, they had concluded, would set the Iranians back considerably. It is unclear who introduced the programming error.

The question facing Mr. Obama was whether the rest of Olympic Games was in jeopardy, now that a variant of the bug was replicating itself “in the wild,” where computer security experts can dissect it and figure out its purpose.

“I don’t think we have enough information,” Mr. Obama told the group that day, according to the officials. But in the meantime, he ordered that the cyberattacks continue. They were his best hope of disrupting the Iranian nuclear program unless economic sanctions began to bite harder and reduced Iran’s oil revenues.

6/1/12

Obama Ordered Wave of Cyberattacks Against Iran - NYTimes.com

Within a week, another version of the bug brought down just under 1,000 centrifuges. Olympic Games was still on.

A Weapon's Uncertain Future

American cyberattacks are not limited to Iran, but the focus of attention, as one administration official put it, "has been overwhelmingly on one country." There is no reason to believe that will remain the case for long. Some officials question why the same techniques have not been used more aggressively against North Korea. Others see chances to disrupt Chinese military plans, forces in Syria on the way to suppress the uprising there, and Qaeda operations around the world. "We've considered a lot more attacks than we have gone ahead with," one former intelligence official said.

Mr. Obama has repeatedly told his aides that there are risks to using — and particularly to overusing — the weapon. In fact, no country's infrastructure is more dependent on computer systems, and thus more vulnerable to attack, than that of the United States. It is only a matter of time, most experts believe, before it becomes the target of the same kind of weapon that the Americans have used, secretly, against Iran.

This article is adapted from "Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power," to be published by Crown on Tuesday.



FREEDOM WATCH

www.FreedomWatchUSA.org

World Headquarters 2020 Pennsylvania Avenue, N.W., Suite 345, Washington, DC 20006-1811 (310) 595-0800 leklayman@gmail.com

FAX

To: Central Intelligence Agency **From:** Freedom Watch

Fax: 703-613-3007 **Pages:** 11 (excluding this one)

Phone: **Date:** 06-01-12

Re: FOIA Request **CC:**

Urgent For Review Please Comment Please Reply

[Handwritten signature]
Freedom Watch

ATTACHMENT 2



Washington, D.C. 20505

12 June 2012

Larry Klayman, Esq.
Chairman and General Counsel
Freedom Watch
2020 Pennsylvania Avenue, NW
Suite 345
Washington, DC 20006

Reference: F-2012-01429

Dear Mr. Klayman:

This is a final response to your 1 June 2012 Freedom of Information Act (FOIA) request, submitted on behalf of Freedom Watch, for all correspondence, documents, or records related to the following in any way:

1. Any and all information that refers or relates to the New York Times article entitled "Obama Order Sped Up Wave of Cyberattacks Against Iran" by David E. Sanger.
2. Any and all information that refers or relates in any way to information released to David E. Sanger and/or made available to him.
3. The names of persons, employers and job titles, and addresses of those who "leaked" the above information to David E. Sanger.
4. Communications with The White House and/or Office of the President and/or Vice President that refer or relate in any way to the "leaked" information and/or the reason for "leaking" the information.
5. Any and all information that refer or relate to the decision to "leak" the above previously classified information.
6. Any and all information that refers or relates to government agencies deciding to investigate who "leaked" the above previously classified information.

In accordance with section 3.6(a) of Executive Order 13526, the CIA can neither confirm nor deny the existence or nonexistence of records responsive to your request. The fact of the existence or nonexistence of requested records is currently and properly classified and is intelligence sources and methods information that is protected from disclosure by section 6 of the CIA Act of 1949, as amended, and section 102A(i)(1) of the National Security Act of 1947, as amended. Therefore, your request is denied pursuant to FOIA exemptions (b)(1) and (b)(3). I

JA66

have enclosed an explanation of these exemptions for your reference and retention. As the CIA Information and Privacy Coordinator, I am the CIA official responsible for this determination. You have the right to appeal this response to the Agency Release Panel, in my care, within 45 days from the date of this letter. Please include the basis of your appeal.

Sincerely,



Michele Meeks
Information and Privacy Coordinator

Enclosure

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

FREEDOM WATCH, INC.,

Plaintiff,

v.

NATIONAL SECURITY AGENCY;
CENTRAL INTELLIGENCE AGENCY;
DEPARTMENT OF DEFENSE; and
DEPARTMENT OF STATE,

Defendants.

Case No. 1:12-cv-01088
Judge Robert L. Wilkins

EXHIBIT C

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

FREEDOM WATCH, INC.,)	
)	
Plaintiff,)	
)	
v.)	Case No. 12-cv-01088
)	Judge Robert L. Wilkins
NATIONAL SECURITY)	
AGENCY, <i>et al.</i> ,)	
)	
Defendants.)	
)	

DECLARATION OF SHERYL L. WALTER

Pursuant to 28 U.S.C. § 1746, I, Sheryl L. Walter, declare and state as follows:

1. I am the Director of the Office of Information Programs and Services (“IPS”) of the United States Department of State (the “Department”). In this capacity, I am the Department official immediately responsible for responding to requests for records under the Freedom of Information Act (“FOIA”), 5 U.S.C. § 552, the Privacy Act, 5 U.S.C. § 552a, and other applicable records access provisions. I have been employed by the Department in this capacity since 2011. I make the following statements based upon my personal knowledge, which in turn is based on a personal review of the records in the case file established for processing the subject request and upon information furnished to me in the course of my official duties.

2. On June 8, 2012, IPS received a FOIA request by mail from Freedom Watch, Inc. (“Plaintiff”) dated June 1, 2012, attached as Exhibit 1. The request sought six categories of records related to information purportedly provided to the author of a June 2012 *New York Times* article. The request also sought both a fee waiver and expedited processing.

3. By letter dated June 27, 2012, attached as Exhibit 2, IPS acknowledged receipt of Plaintiff's FOIA request and assigned it Case Control Number F-2012-28257. The letter notified Plaintiff that the Department would begin processing its FOIA request.

4. The letter also explained that a decision on whether to grant or deny Plaintiff's request for a fee waiver would be deferred "until [the Department is] able to determine whether the disclosure of any records responsive to [Plaintiff's] request is in the public interest."

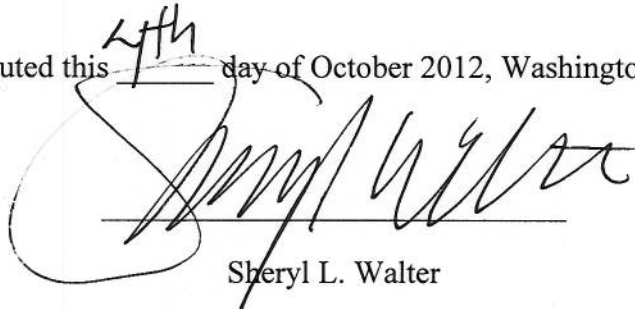
5. The letter further stated that Plaintiff's request for expedited processing was denied because Plaintiff did not provide adequate justification for expedition. Appeal rights were granted for the denial and a copy of the Department's expedited processing criteria was enclosed.

6. I have identified fundamental deficiencies in Plaintiff's FOIA request, which the Department has not yet begun processing. Each item of Plaintiff's request appears to be based on the proposition that the Department has "provided and leaked" information to David Sanger and/or the *New York Times* as background for the June 2012 article. Therefore, responding to Plaintiff's request would necessarily require the Department to investigate whether any information was "provided and leaked" to Mr. Sanger and/or the *New York Times*.

7. I declare under penalty of perjury that the foregoing is true and correct.

* * *

Executed this 4th day of October 2012, Washington, D.C.



Sheryl L. Walter

ATTACHMENT 1



FREEDOM WATCH

► www.FreedomWatchUSA.org

► World Headquarters 2020 Pennsylvania Avenue, N.W., Suite 345, Washington, DC 20006-1811 ► (310) 595-0800 ► leklayman@gmail.com

Via Mail and Fax

June 1, 2012

Office of Information Programs and Services
A/GIS/IPS/RL
U. S. Department of State
Washington, D. C. 20522-8100

Re: Freedom of Information Act Request

Dear Sir/Madam:

On June 1, 2012, the New York Times published two articles, "Obama Order Sped Up Wave of Cyberattacks Against Iran" by David E. Sanger. This article, a copy of which is attached, relied in large part on previously classified information which was released by Obama administration sources on the President's behalf. This released information is thus no longer classified and is no longer exempt from being released pursuant to the Freedom of Information Act. 5 U.S.C. 552 et seq.

Pursuant to the Freedom of Information Act (5 U.S.C. § 552 et seq.), Freedom Watch requests that that the Department of State produce all correspondence, memoranda, documents, reports, records, statements, audits, lists of names, applications, diskettes, letters, expense logs and receipts, calendar or diary logs, facsimile logs, telephone records call sheets, tape recordings, video/movie recordings, notes, examinations, opinions, folders, files, books, manuals, pamphlets, forms, drawings, charts, photographs, electronic mail, and other documents and things (hereinafter, "information") that refer or relate to the following in any way, within ten (10) business days as set forth below:

- 1) Any and all information that refers or relates to the New York Times article entitled "Obama Order Sped Up Wave of Cyberattacks Against Iran" by David E. Sanger on Friday, June 1, 2012, and which information was provided and leaked to Mr. Sanger and the New York Times;
- 2) Any and all information that refers or relates in any way to information released to David E. Sanger and/or made available to him;
- 3) The names of the persons, employers and job titles, and addresses of those who "leaked" the above information to David E. Sanger

'12 JUN 8 PM 1:57

WALTER DECLARATION
Civil Action No. 1:12-cv-01088-RLW
Exhibit 1

JA72

State Department
FOIA Request
Page | 2

- 4) Communications with The White House and/or Office of the President and/or Vice President that refer or relate in any way to the "leaked" information and/or the reasons for "leaking" the information;
- 5) Any and all information that refer or relate to the decision to "leak" the above previously classified information;
- 6) Any and all information that refers or relates to government agencies deciding to investigate who "leaked" the above previously classified information.

If any responsive record or portion thereof is claimed to be exempt from production under FOIA, sufficient identifying information (with respect to each allegedly exempt record or portion thereof) must be provided to allow the assessment of the propriety of the claimed exemption. *Vaughn v. Rosen*, 484 F.2d 820 (D.C. Cir. 1973), *cert denied*, 415 U.S. 977 (1974). Additionally, pursuant to law, any reasonably segregable portion of a responsive record must be provided after redaction of any allegedly exempt material. 5 U.S.C. §552(b).

I request a waiver of all fees for this request under 5. U.S.C. § 552(a)(4)(A)(iii). Disclosure of the requested information to Freedom Watch is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in my commercial interest. The Islamic Republic of Iran's goal of obtaining nuclear weapons affects the safety of both Israel and the United States, thus putting American citizens at risk. Furthermore, the release of classified information by any particular individual within the executive branch, including the president, further endangers the American people and raises a spectre of corruption within the federal government that must be examined. Freedom Watch is engaged in the active dissemination of public information as is evident by our ongoing public interest legal work and continual fight against corruption within the United States government, and international cases, particularly with regard to Iran. Freedom Watch's website, freedomwatchusa.org serves as the primary means of disseminating that information, and is seen by millions of people annually. In addition, officials of Freedom Watch frequently appear on radio and television to disseminate important information to the public.

Furthermore, on behalf of Freedom Watch I am requesting expedited handling as provided in 6 C.F.R. 5.5(d) because there is an urgency to inform the public about an actual or alleged federal government activity. Iran is reportedly on the verge of acquiring nuclear weapons and Israel is reportedly on the verge of attacking it to prevent their acquisition. The issue of a possible attack on Iran is of importance to the American people because Iran's acquiring of nuclear weapons places the safety of the American

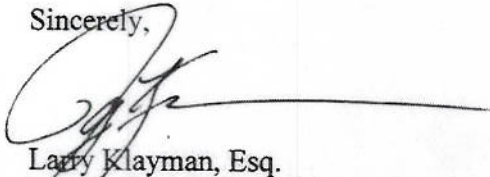
State Department
FOIA Request
Page | 3

people as well as the safety of our allies in jeopardy. This war can break out any time because a strike is needed before Iran can gain the capability to build a bomb. This fact is also evidenced in the article mentioned above. There is an immediate clear and present danger to U.S. citizens, American military personnel.

The above mentioned "leaked" information is no longer in effect classified, if it ever was, as it was disclosed to the public by Mr. Sanger and The New York Times with the aid and complicity of President Obama and his administration. It was disclosed for political purposes to further President Obama's 2012 re-election campaign.

On behalf of Freedom Watch, I look forward to receiving the requested documents and a full fee waiver within ten (10) business days. You may have them delivered to the above address.

Sincerely,



Larry Klayman, Esq.
Chairman and General Counsel
2020 Pennsylvania Ave, N.W., Suite 345
Washington, D.C. 20006
leklayman@gmail.com

The New York Times

June 1, 2012

Obama Order Sped Up Wave of Cyberattacks Against Iran

By DAVID E. SANGER

WASHINGTON — From his first months in office, President Obama secretly ordered increasingly sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, significantly expanding America's first sustained use of cyberweapons, according to participants in the program.

Mr. Obama decided to accelerate the attacks — begun in the Bush administration and code-named Olympic Games — even after an element of the program accidentally became public in the summer of 2010 because of a programming error that allowed it to escape Iran's Natanz plant and sent it around the world on the Internet. Computer security experts who began studying the worm, which had been developed by the United States and Israel, gave it a name: Stuxnet.

At a tense meeting in the White House Situation Room within days of the worm's "escape," Mr. Obama, Vice President Joseph R. Biden Jr. and the director of the Central Intelligence Agency at the time, Leon E. Panetta, considered whether America's most ambitious attempt to slow the progress of Iran's nuclear efforts had been fatally compromised.

"Should we shut this thing down?" Mr. Obama asked, according to members of the president's national security team who were in the room.

Told it was unclear how much the Iranians knew about the code, and offered evidence that it was still causing havoc, Mr. Obama decided that the cyberattacks should proceed. In the following weeks, the Natanz plant was hit by a newer version of the computer worm, and then another after that. The last of that series of attacks, a few weeks after Stuxnet was detected around the world, temporarily took out nearly 1,000 of the 5,000 centrifuges Iran had spinning at the time to purify uranium.

This account of the American and Israeli effort to undermine the Iranian nuclear program is based on interviews over the past 18 months with current and former American, European and Israeli officials involved in the program, as well as a range of outside experts. None would allow

their names to be used because the effort remains highly classified, and parts of it continue to this day.

These officials gave differing assessments of how successful the sabotage program was in slowing Iran's progress toward developing the ability to build nuclear weapons. Internal Obama administration estimates say the effort was set back by 18 months to two years, but some experts inside and outside the government are more skeptical, noting that Iran's enrichment levels have steadily recovered, giving the country enough fuel today for five or more weapons, with additional enrichment.

Whether Iran is still trying to design and build a weapon is in dispute. The most recent United States intelligence estimate concludes that Iran suspended major parts of its weaponization effort after 2003, though there is evidence that some remnants of it continue.

Iran initially denied that its enrichment facilities had been hit by Stuxnet, then said it had found the worm and contained it. Last year, the nation announced that it had begun its own military cyberunit, and Brig. Gen. Gholamreza Jalali, the head of Iran's Passive Defense Organization, said that the Iranian military was prepared "to fight our enemies" in "cyberspace and Internet warfare." But there has been scant evidence that it has begun to strike back.

The United States government only recently acknowledged developing cyberweapons, and it has never admitted using them. There have been reports of one-time attacks against personal computers used by members of Al Qaeda, and of contemplated attacks against the computers that run air defense systems, including during the NATO-led air attack on Libya last year. But Olympic Games was of an entirely different type and sophistication.

It appears to be the first time the United States has repeatedly used cyberweapons to cripple another country's infrastructure, achieving, with computer code, what until then could be accomplished only by bombing a country or sending in agents to plant explosives. The code itself is 50 times as big as the typical computer worm, Carey Nachenberg, a vice president of Symantec, one of the many groups that have dissected the code, said at a symposium at Stanford University in April. Those forensic investigations into the inner workings of the code, while picking apart how it worked, came to no conclusions about who was responsible.

A similar process is now under way to figure out the origins of another cyberweapon called Flame that was recently discovered to have attacked the computers of Iranian officials, sweeping up information from those machines. But the computer code appears to be at least five years old, and American officials say that it was not part of Olympic Games. They have declined to say whether the United States was responsible for the Flame attack.

Mr. Obama, according to participants in the many Situation Room meetings on Olympic Games, was acutely aware that with every attack he was pushing the United States into new territory, much as his predecessors had with the first use of atomic weapons in the 1940s, of intercontinental missiles in the 1950s and of drones in the past decade. He repeatedly expressed concerns that any American acknowledgment that it was using cyberweapons — even under the most careful and limited circumstances — could enable other countries, terrorists or hackers to justify their own attacks.

“We discussed the irony, more than once,” one of his aides said. Another said that the administration was resistant to developing a “grand theory for a weapon whose possibilities they were still discovering.” Yet Mr. Obama concluded that when it came to stopping Iran, the United States had no other choice.

If Olympic Games failed, he told aides, there would be no time for sanctions and diplomacy with Iran to work. Israel could carry out a conventional military attack, prompting a conflict that could spread throughout the region.

A Bush Initiative

The impetus for Olympic Games dates from 2006, when President George W. Bush saw few good options in dealing with Iran. At the time, America’s European allies were divided about the cost that imposing sanctions on Iran would have on their own economies. Having falsely accused Saddam Hussein of reconstituting his nuclear program in Iraq, Mr. Bush had little credibility in publicly discussing another nation’s nuclear ambitions. The Iranians seemed to sense his vulnerability, and, frustrated by negotiations, they resumed enriching uranium at an underground site at Natanz, one whose existence had been exposed just three years before.

Iran’s president, Mahmoud Ahmadinejad, took reporters on a tour of the plant and described grand ambitions to install upward of 50,000 centrifuges. For a country with only one nuclear power reactor — whose fuel comes from Russia — to say that it needed fuel for its civilian nuclear program seemed dubious to Bush administration officials. They feared that the fuel could be used in another way besides providing power: to create a stockpile that could later be enriched to bomb-grade material if the Iranians made a political decision to do so.

Hawks in the Bush administration like Vice President Dick Cheney urged Mr. Bush to consider a military strike against the Iranian nuclear facilities before they could produce fuel suitable for a weapon. Several times, the administration reviewed military options and concluded that they would only further inflame a region already at war, and would have uncertain results.

For years the C.I.A. had introduced faulty parts and designs into Iran’s systems — even

6/1/12

Obama Ordered Wave of Cyberattacks Against Iran - NYTimes.com

tinkering with imported power supplies so that they would blow up — but the sabotage had had relatively little effect. General James E. Cartwright, who had established a small cyberoperation inside the United States Strategic Command, which is responsible for many of America’s nuclear forces, joined intelligence officials in presenting a radical new idea to Mr. Bush and his national security team. It involved a far more sophisticated cyberweapon than the United States had designed before.

The goal was to gain access to the Natanz plant’s industrial computer controls. That required leaping the electronic moat that cut the Natanz plant off from the Internet — called the air gap, because it physically separates the facility from the outside world. The computer code would invade the specialized computers that command the centrifuges.

The first stage in the effort was to develop a bit of computer code called a beacon that could be inserted into the computers, which were made by the German company Siemens and an Iranian manufacturer, to map their operations. The idea was to draw the equivalent of an electrical blueprint of the Natanz plant, to understand how the computers control the giant silvery centrifuges that spin at tremendous speeds. The connections were complex, and unless every circuit was understood, efforts to seize control of the centrifuges could fail.

Eventually the beacon would have to “phone home” — literally send a message back to the headquarters of the National Security Agency that would describe the structure and daily rhythms of the enrichment plant. Expectations for the plan were low; one participant said the goal was simply to “throw a little sand in the gears” and buy some time. Mr. Bush was skeptical, but lacking other options, he authorized the effort.

Breakthrough, Aided by Israel

It took months for the beacons to do their work and report home, complete with maps of the electronic directories of the controllers and what amounted to blueprints of how they were connected to the centrifuges deep underground.

Then the N.S.A. and a secret Israeli unit respected by American intelligence of cyberskills set to work developing the enormously complex computer worm that the attacker from within.

MORE IN MI

Egypt A Verdict

[Read More](#)

The unusually tight collaboration with Israel was driven by two imperatives. I... a part of its military, had technical expertise that rivaled the N.S.A.’s, and the Israelis had deep intelligence about operations at Natanz that would be vital to making the cyberattack a success. But American officials had another interest, to dissuade the Israelis from carrying out their own pre-emptive strike against the Iranian nuclear facilities. To do that, the Israelis would have to

be convinced that the new line of attack was working. The only way to convince them, several officials said in interviews, was to have them deeply involved in every aspect of the program.

Soon the two countries had developed a complex worm that the Americans called “the bug.” But the bug needed to be tested. So, under enormous secrecy, the United States began building replicas of Iran’s P-1 centrifuges, an aging, unreliable design that Iran purchased from Abdul Qadeer Khan, the Pakistani nuclear chief who had begun selling fuel-making technology on the black market. Fortunately for the United States, it already owned some P-1s, thanks to the Libyan dictator, Col. Muammar el-Qaddafi.

When Colonel Qaddafi gave up his nuclear weapons program in 2003, he turned over the centrifuges he had bought from the Pakistani nuclear ring, and they were placed in storage at a weapons laboratory in Tennessee. The military and intelligence officials overseeing Olympic Games borrowed some for what they termed “destructive testing,” essentially building a virtual replica of Natanz, but spreading the test over several of the Energy Department’s national laboratories to keep even the most trusted nuclear workers from figuring out what was afoot.

Those first small-scale tests were surprisingly successful: the bug invaded the computers, lurking for days or weeks, before sending instructions to speed them up or slow them down so suddenly that their delicate parts, spinning at supersonic speeds, self-destructed. After several false starts, it worked. One day, toward the end of Mr. Bush’s term, the rubble of a centrifuge was spread out on the conference table in the Situation Room, proof of the potential power of a cyberweapon. The worm was declared ready to test against the real target: Iran’s underground enrichment plant.

“Previous cyberattacks had effects limited to other computers,” Michael V. Hayden, the former chief of the C.I.A., said, declining to describe what he knew of these attacks when he was in office. “This is the first attack of a major nature in which a cyberattack was used to effect physical destruction,” rather than just slow another computer, or hack into it to steal data.

“Somebody crossed the Rubicon,” he said.

Getting the worm into Natanz, however, was no easy trick. The United States and Israel would have to rely on engineers, maintenance workers and others — both spies and unwitting accomplices — with physical access to the plant. “That was our holy grail,” one of the architects of the plan said. “It turns out there is always an idiot around who doesn’t think much about the thumb drive in their hand.”

In fact, thumb drives turned out to be critical in spreading the first variants of the computer worm; later, more sophisticated methods were developed to deliver the malicious code.

The first attacks were small, and when the centrifuges began spinning out of control in 2008, the Iranians were mystified about the cause, according to intercepts that the United States later picked up. "The thinking was that the Iranians would blame bad parts, or bad engineering, or just incompetence," one of the architects of the early attack said.

The Iranians were confused partly because no two attacks were exactly alike. Moreover, the code would lurk inside the plant for weeks, recording normal operations; when it attacked, it sent signals to the Natanz control room indicating that everything downstairs was operating normally. "This may have been the most brilliant part of the code," one American official said.

Later, word circulated through the International Atomic Energy Agency, the Vienna-based nuclear watchdog, that the Iranians had grown so distrustful of their own instruments that they had assigned people to sit in the plant and radio back what they saw.

"The intent was that the failures should make them feel they were stupid, which is what happened," the participant in the attacks said. When a few centrifuges failed, the Iranians would close down whole "stands" that linked 164 machines, looking for signs of sabotage in all of them. "They overreacted," one official said. "We soon discovered they fired people."

Imagery recovered by nuclear inspectors from cameras at Natanz — which the nuclear agency uses to keep track of what happens between visits — showed the results. There was some evidence of wreckage, but it was clear that the Iranians had also carted away centrifuges that had previously appeared to be working well.

But by the time Mr. Bush left office, no wholesale destruction had been accomplished. Meeting with Mr. Obama in the White House days before his inauguration, Mr. Bush urged him to preserve two classified programs, Olympic Games and the drone program in Pakistan. Mr. Obama took Mr. Bush's advice.

The Stuxnet Surprise

Mr. Obama came to office with an interest in cyberissues, but he had discussed them during the campaign mostly in terms of threats to personal privacy and the risks to infrastructure like the electrical grid and the air traffic control system. He commissioned a major study on how to improve America's defenses and announced it with great fanfare in the East Room.

What he did not say then was that he was also learning the arts of cyberwar. The architects of Olympic Games would meet him in the Situation Room, often with what they called the "horse blanket," a giant foldout schematic diagram of Iran's nuclear production facilities. Mr. Obama authorized the attacks to continue, and every few weeks — certainly after a major attack — he

would get updates and authorize the next step. Sometimes it was a strike riskier and bolder than what had been tried previously.

“From his first days in office, he was deep into every step in slowing the Iranian program — the diplomacy, the sanctions, every major decision,” a senior administration official said. “And it’s safe to say that whatever other activity might have been under way was no exception to that rule.”

But the good luck did not last. In the summer of 2010, shortly after a new variant of the worm had been sent into Natanz, it became clear that the worm, which was never supposed to leave the Natanz machines, had broken free, like a zoo animal that found the keys to the cage. It fell to Mr. Panetta and two other crucial players in Olympic Games — General Cartwright, the vice chairman of the Joint Chiefs of Staff, and Michael J. Morell, the deputy director of the C.I.A. — to break the news to Mr. Obama and Mr. Biden.

An error in the code, they said, had led it to spread to an engineer’s computer when it was hooked up to the centrifuges. When the engineer left Natanz and connected the computer to the Internet, the American- and Israeli-made bug failed to recognize that its environment had changed. It began replicating itself all around the world. Suddenly, the code was exposed, though its intent would not be clear, at least to ordinary computer users.

“We think there was a modification done by the Israelis,” one of the briefers told the president, “and we don’t know if we were part of that activity.”

Mr. Obama, according to officials in the room, asked a series of questions, fearful that the code could do damage outside the plant. The answers came back in hedged terms. Mr. Biden fumed. “It’s got to be the Israelis,” he said. “They went too far.”

In fact, both the Israelis and the Americans had been aiming for a particular part of the centrifuge plant, a critical area whose loss, they had concluded, would set the Iranians back considerably. It is unclear who introduced the programming error.

The question facing Mr. Obama was whether the rest of Olympic Games was in jeopardy, now that a variant of the bug was replicating itself “in the wild,” where computer security experts can dissect it and figure out its purpose.

“I don’t think we have enough information,” Mr. Obama told the group that day, according to the officials. But in the meantime, he ordered that the cyberattacks continue. They were his best hope of disrupting the Iranian nuclear program unless economic sanctions began to bite harder and reduced Iran’s oil revenues.

Within a week, another version of the bug brought down just under 1,000 centrifuges. Olympic Games was still on.

A Weapon's Uncertain Future

American cyberattacks are not limited to Iran, but the focus of attention, as one administration official put it, "has been overwhelmingly on one country." There is no reason to believe that will remain the case for long. Some officials question why the same techniques have not been used more aggressively against North Korea. Others see chances to disrupt Chinese military plans, forces in Syria on the way to suppress the uprising there, and Qaeda operations around the world. "We've considered a lot more attacks than we have gone ahead with," one former intelligence official said.

Mr. Obama has repeatedly told his aides that there are risks to using — and particularly to overusing — the weapon. In fact, no country's infrastructure is more dependent on computer systems, and thus more vulnerable to attack, than that of the United States. It is only a matter of time, most experts believe, before it becomes the target of the same kind of weapon that the Americans have used, secretly, against Iran.

This article is adapted from "Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power," to be published by Crown on Tuesday.

ATTACHMENT 2



United States Department of State

Washington, D.C. 20520

June 27, 2012

Larry Klayman
2020 Pennsylvania Ave, NW., Ste 345
Washington, DC 20006

RE: Obama order sped up wave of cyber attacks against Iran by David E. Sanger.

Dear Mr. Klayman:

This is in response to your request dated June 01, 2012. We have assigned Case Control Number F-2012-28257 and will begin the processing of your request based upon the information provided in your communication.

The cut-off date is the date the search is initiated unless you have provided a specific timeframe.

We have considered your request of a fee waiver. A waiver or reduction of fees may be appropriate when the disclosure of records is in the public interest because the disclosure is likely to contribute significantly to public understanding of the operations or activities of the Government and is not primarily in the interest of the requester. See 22 C.F.R. § 171.17. In light of the information supplied in your request, we will now defer our decision to grant or deny your request for a fee waiver until we are able to determine whether the disclosure of any records responsive to your request is in the public interest, consistent with the application of 22 C.F.R. § 171.17.

Our published regulations regarding expedition, 22 C.F.R. § 171.12(b), require a specific showing of a compelling need. **Expedited processing is granted only in the following situations: (1) imminent threat to the life or physical safety of an individual; (2) urgently needed by an individual primarily engaged in disseminating information in order to inform the public concerning actual or alleged Federal Government activity and the information is urgently needed in that a particular value of the information would be lost if not disseminated quickly; (3) substantial humanitarian reasons; and (4) loss of substantial due process rights.** Your request does not meet any of the established criteria. Regrettably, I must advise that you have not provided adequate justification for expedition. However, you may be assured that we will make every effort to process your request in as timely a manner as possible. For your convenience, I have enclosed a copy of the Department's expeditious processing criteria.

If you wish to appeal the denial of expedition, you may write to the Chief, Requester Liaison Division, at the address below, within 30 days of receipt of this letter.

Office of Information Programs and Services
U.S. Department of State, SA-2
Washington, DC 20522-8100
Website: www.foia.state.gov

Inquiries:
Phone: 1-202-261-8484
FAX: 1-202-261-8579
E-mail: FOIAStatus@state.gov

WALTER DECLARATION
Civil Action No. 1:12-cv-01088-RLW
Exhibit 2

JA84

Unusual circumstances (including the number and location of Department components involved in responding to your request, the volume of requested records, etc.) may arise that would require additional time to process your request.

We will notify you as soon as responsive material has been retrieved and reviewed. Should you want to contact us, you may call our FOIA Requester Service Center at (202) 261-8484 or send an email to FOIAstatus@state.gov. Please refer to the Case Control Number in any communication.

Sincerely,



Mary Therese Casto
Chief, Requester Communications Branch

Fees: The Freedom of Information Act (FOIA) provides that agencies may assess fees to recover the direct costs of processing requests, unless a fee waiver has been granted.

According to our regulations, by making a FOIA request, you have agreed to pay all applicable fees up to \$25 unless a fee waiver has been granted. You may specify a willingness to pay a greater amount. If the estimated fees exceed this limit, you will be notified.

___ You have stated your willingness to pay the fees incurred in the processing of this request up to \$___.

X Please let us know if you are willing to pay the fees that will be incurred in the processing of your request. You may set a limit of the maximum amount that you wish to pay. Please be advised that, without an agreement to pay fees, your request will be processed without cost up to the required first 2 hours of search time (for all other requester category only) and duplication of the first 100 pages (for all other, media, educational and non-commercial scientific requester categories).

Based upon the information that you have provided, we have placed you in the requester category checked below. This request will be processed in accordance with the fee schedule designated for that category (see 22 C.F.R. 171, enclosed).

___ **Commercial Use Requesters** – Charges may be assessed that recover the full direct costs of searching for, reviewing for release, and duplicating the record(s) sought.

___ **Educational Institution Requesters** – Charges may be assessed that recover the cost of duplicating the record(s) sought only, after the first 100 pages of duplication.

___ **Non-commercial Scientific Institution Requesters** – Charges may be assessed that recover the cost of duplicating the record(s) sought only, after the first 100 pages of duplication.

X **Representatives of the News Media** – Charges may be assessed that recover the cost of duplicating the record(s) sought only, after the first 100 pages of duplication.

___ **All Other Requesters** – Charges may be assessed that recover the full reasonable direct cost of searching for and duplicating the record(s) sought, after the first 100 pages of duplication, and the first two hours of search time.

___ You have indicated your inclusion in a category different than the one indicated above. Please forward the information requested on the enclosed sheet titled “Requester Categories” to substantiate your inclusion in a particular category of requester.

We will notify you of the costs incurred in processing your request as soon as the search for, and review of, any responsive documents have been completed.

Office of Information Programs and Services
U.S. Department of State, SA-2
Washington, DC 20522-8100
Website: www.foia.state.gov

Inquiries:
Phone: 1-202-261-8484
FAX: 1-202-261-8579
E-mail: FOIAStatus@state.gov

Expedited Processing Information Sheet

Expedited processing shall be granted to a requester after the requester requests such and demonstrates a compelling need for the information. A compelling need is deemed to exist where the requester can demonstrate one of the following:

1. **A Compelling Need** means that the failure to obtain the records on an expedited basis could reasonably be expected to pose an imminent threat to the life or physical safety of an individual.
2. **A Compelling Need** means that the information is urgently needed by an individual primarily engaged in disseminating information in order to inform the public concerning actual or alleged Federal Government activity. An individual primarily engaged in disseminating information to the public. Representatives of the news media would normally qualify; however, other persons must demonstrate that their primary activity involves publishing or otherwise disseminating information to the public, not just to a particular segment or group.
 - (a) **Urgently Needed** means that the information has a particular value that will be lost if not disseminated quickly. Ordinarily this means a breaking news story of historical interest only, or information sought for litigation or commercial activities would not qualify nor would a news media publication or broadcast deadline unrelated to the news breaking nature of the information.
 - (b) **Actual or Alleged Federal Government Activity.** The information concerns some actions taken, contemplated, or alleged by or about the Government of the United States, or one of its components or agencies, including the Congress.
3. **Substantial Due Process** rights of the requester would be impaired by the failure to process immediately; or
4. **Substantial Humanitarian** concerns would be harmed by the failure to process immediately.

A demonstration of compelling need by a requester shall be made by a statement certified by the requester to be true and correct to the best of their knowledge.

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

FREEDOM WATCH, INC.,

Plaintiff,

v.

NATIONAL SECURITY AGENCY;
CENTRAL INTELLIGENCE AGENCY;
DEPARTMENT OF DEFENSE; and
DEPARTMENT OF STATE,

Defendants.

Case No. 1:12-cv-01088
Judge Robert L. Wilkins

EXHIBIT D

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

FREEDOM WATCH, INC.)	
)	
Plaintiff,)	
)	
v.)	
)	Civil Action No.: 1:12-cv-01088
NATIONAL SECURITY AGENCY, <i>et. al.</i>)	
)	
Defendants)	
)	

DECLARATION OF VICE ADMIRAL KURT W. TIDD

I, Kurt W. Tidd, Vice Admiral, United States Navy, pursuant to 28 U.S.C. § 1746 make the following declaration.

1. I am the Director of Operations for the Joint Staff at the Pentagon and have served in this capacity since July 27, 2012. In my capacity as the Director of Operations I am responsible for all Department of Defense (DoD) operational matters outside of the continental United States. As such, I coordinate and communicate frequently with the staffs of the Unified Combatant Commands, to include U.S. Africa Command, U.S. Central Command, U.S. European Command, U.S. Pacific Command, U.S. Southern Command, U.S. Strategic Command, U.S. Transportation Command and U.S. Special Operations Command, as well as with the Intelligence Community, to ensure on behalf of the Chairman of the Joint Chief of Staff that the President of the United States' and Secretary of Defense's direction and guidance are conveyed and executed, and that combatant command concerns are addressed by the Joint Staff. I evaluate and synthesize such concerns and advise and make recommendations to the Chairman of the Joint Chiefs of Staff regarding our worldwide military operations. I have served in the United States Armed Forces for over thirty

years at various levels of command and staff. As a commander of U.S. forces, I commanded U.S. Naval Forces Southern Command and U.S. 4th Fleet, Carrier Strike Group 8 aboard USS *Dwight D. Eisenhower* (CVN 69) (during a combat deployment supporting coalition forces in Operation Enduring Freedom), and Persian Gulf maritime operations as Commander, Middle East Force and Commander Task Force 55. As the Director of Operations, I receive and review daily operational plans and briefings, reports and intelligence analyses from the Combatant Commands, the Joint Staff, and the Intelligence Community.

2. I make the following statements based upon my years of service and experience in the United States military, personal knowledge, and information made available to me in my official capacity.

3. I am familiar with the above captioned litigation and the FOIA request, dated June 1, 2012, which plaintiff sent to multiple defendants, including DoD, seeking records regarding a *New York Times* article regarding cyber-attacks against Iran. A copy of the request is attached as Exhibit 1. The request appears to seek information that refers or relates in any way to the contents of the *New York Times* article. The article discusses “attacks on the computer systems that run Iran’s main nuclear enrichment facilities” allegedly conducted by the United States. The article also refers to alleged military operations and intelligence gathering efforts implicating several foreign nations, including Israel, Libya, and Pakistan.

4. By letter dated June 7, 2012, DoD acknowledged receipt of Plaintiff’s FOIA request. A copy of DoD’s June 7, 2012 letter is attached as Exhibit 2.

5. By letter dated October 1, 2012, DoD informed Plaintiff that “the fact of the existence or nonexistence of documents concerning the matters relating to those set forth in your request is classified in accordance with Executive Order 13526.” A copy of DoD’s October 1,

2012 letter to Plaintiff is attached as Exhibit 3. This response is commonly referred to as a *Glomar* response.

6. The purpose of this declaration is to articulate the basis for the DoD *Glomar* response Plaintiff's FOIA request.

7. FOIA exemption 1, 5 U.S.C. § 552(b)(1), provides that the FOIA disclosure provisions do not apply to matters that are: (A) specifically authorized under criteria established by an Executive Order to be kept from disclosure in the interests of national defense or foreign policy; and (B) are in fact properly classified pursuant to such an Executive Order.

8. Executive Order (E.O.) 13526 establishes a framework for "classifying" and "safeguarding" national security information, Section 6.1(i) of E.O. 13526 defines "classified national security information" or "classified information" as "information that has been determined pursuant to this order or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form." Section 6.1(ec) of E.O. 13526 defines "national security" as the "national defense or foreign relations of the United States."

9. Section 1.1(a) of E.O. 13526 provides that information may be originally classified under the terms of this order only if all of the following conditions are met: (1) an original classification authority is classifying the information; (2) the information is owned by, produced by or for, or is under the control of the U.S. government; (3) the information falls within one or more of the categories of information listed in section 1.4 of E.O. 13526; and (4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in some level of damage to the national security and the original classification authority is able to identify or describe the damage.

10. In Section 1.3(a)(2) of E.O. 13526, the President authorized agency heads to designate officials that may classify information originally as TOP SECRET. In turn, and pursuant to Section 1.3 (e) of E.O. 13526, the Deputy Secretary of Defense, acting pursuant to a delegation from the Secretary of Defense, has authorized me to exercise TOP SECRET original classification authority.

11. Section 3.6(a) of E.O. 13526 specifically states that “an agency may refuse to confirm or deny the existence or non-existence of requested records whenever the fact of their existence or non-existence is itself classified under this order or its predecessors.”

12. As an original classification authority, consistent with Sections 1.1(a) and 3.6(a) of E.O. 13526, and as described below, I have determined that the fact of the existence or nonexistence of the records requested in plaintiffs request is a properly classified fact that concerns E.O. 13526 Sections 1.4(a) (military plans, weapons systems, or operations), (d) (foreign relations of the U.S.), and (e) (intelligence activities and intelligence sources and methods).

13. I also have determined that the fact of the existence or non-existence of the requested records has not been classified in order to conceal violations of law, inefficiency, administrative error; prevent embarrassment to a person, organization, or agency; restrain competition; or prevent or delay the release of information that does not require protection in the interests of national security.

14. Acknowledging the existence or non-existence of records responsive to plaintiff’s request could reveal whether the United States, and specifically DoD, conducts or has conducted cyber-attacks against Iran. Accordingly, acknowledging the existence or non-existence of responsive records could clearly reveal military plans, weapons systems, operations, and intelligence activities. Official acknowledgement that DoD has or has not conducted or intends to

conduct a particular military or intelligence activity in Iran would directly impede potential future military or intelligence actions. Such a disclosure would also cause damage to national security by providing insight into DoD's military and intelligence capabilities and interests.

15. In addition, because the request may seek information related to military operations and intelligence activities conducted in coordination with other nations, acknowledging the existence or non-existence of records responsive to Plaintiff's request could reveal the nature and scope of the activities with these foreign nations, and would therefore invariably implicate foreign relations of the U.S. Any response by DoD that could be seen as a confirmation or denial of its alleged involvement in the alleged cyber-attacks could raise questions with other countries about whether or not the DoD is operating clandestinely inside their borders. Although it is known that DoD conducts military and intelligence operations in foreign nations, publicly disclosing a particular military or intelligence activity could cause the foreign government to respond in ways that would damage U.S. national interests.

16. In a typical case, a FOIA requester submits a request to DoD for information on a particular subject and DoD responds by conducting a search for records. If records are located, DoD will provide non-exempt records and those portions of records that can be produced. In the typical case, DoD confirms the existence or non-existence of records. Generally, such confirmation poses no harm to the national security or to intelligence sources and methods because the response focuses on releasing or withholding specific, substantive information. In such cases, the fact that DoD may possess or not possess records is not in itself a classified fact.

17. However, when, as here, the fact of the existence or non-existence of the requested records is classified and reasonably could reveal military and intelligence activities, DoD cannot confirm or deny whether it possesses such information. In other words, what is classified is not

just individual records themselves on a document by document basis, but the mere fact of whether or not DoD does or does not possess responsive records that pertains to plaintiff's request. Any response other than a *Glomar* response could reveal military plans, weapons systems, operations, and intelligence activities, and would clearly implicate foreign relations of the U.S.

18. In order to be credible and effective, DoD must use the *Glomar* response consistently in cases where the existence or non-existence of requested records is a classified fact, including those instances in which DoD does not possess records in response to a particular request. If DoD were to invoke a *Glomar* response only when it possessed responsive records, and inform requesters when it had no records, the *Glomar* response would be interpreted as an admission that responsive records exist. This practice would reveal the very information that DoD was attempting to protect, provide a valuable advantage to foreign intelligence services and endanger DoD's activities worldwide.

19. I declare under penalty of perjury pursuant to 28 U.S.C. § 1746 that the foregoing is true and correct.

Executed this 4TH day of October 2012 in Arlington, VA.



Vice Admiral Kurt W. Tidd, USN
Director of Operations, J-3, Joint Staff

ATTACHMENT 1

12-f-0966



FREEDOM WATCH

www.FreedomWatchUSA.org

World Headquarters 2020 Pennsylvania Avenue, N.W., Suite 345, Washington, DC 20006-1811 (310) 595-0800 lekeyman@gmail.com

Via Mail and Fax

June 1, 2012

OSD/JS FOIA Requester Service Center
Office of Freedom of Information
1155 Defense Pentagon
Washington, DC 20301-1155

Re: Freedom of Information Act Request

Dear Sir/Madam:

On June 1, 2012, the New York Times published two articles, "Obama Order Sped Up Wave of Cyberattacks Against Iran" by David E. Sanger. This article, a copy of which is attached, relied in large part on previously classified information which was released by Obama administration sources on the President's behalf. This released information is thus no longer classified and is no longer exempt from being released pursuant to the Freedom of Information Act. 5 U.S.C. 552 et seq.

Pursuant to the Freedom of Information Act (5 U.S.C. § 552 et seq.), Freedom Watch requests that that the Department of Defense produce all correspondence, memoranda, documents, reports, records, statements, audits, lists of names, applications, diskettes, letters, expense logs and receipts, calendar or diary logs, facsimile logs, telephone records call sheets, tape recordings, video/movie recordings, notes, examinations, opinions, folders, files, books, manuals, pamphlets, forms, drawings, charts, photographs, electronic mail, and other documents and things (hereinafter, "information") that refer or relate to the following in any way, within ten (10) business days as set forth below:

- 1) Any and all information that refers or relates to the New York Times article entitled "Obama Order Sped Up Wave of Cyberattacks Against Iran" by David E. Sanger on Friday, June 1, 2012, and which information was provided and leaked to Mr. Sanger and the New York Times;
- 2) Any and all information that refers or relates in any way to information released to David E. Sanger and/or made available to him;

Defense Department
FOIA Request
Page | 2

- 3) The names of the persons, employers and job titles, and addresses of those who “leaked” the above information to David E. Sanger
- 4) Communications with The White House and/or Office of the President and/or Vice President that refer or relate in any way to the “leaked” information and/or the reasons for “leaking” the information;
- 5) Any and all information that refer or relate to the decision to “leak” the above previously classified information;
- 6) Any and all information that refers or relates to government agencies deciding to investigate who “leaked” the above previously classified information.

If any responsive record or portion thereof is claimed to be exempt from production under FOIA, sufficient identifying information (with respect to each allegedly exempt record or portion thereof) must be provided to allow the assessment of the propriety of the claimed exemption. *Vaughn v. Rosen*, 484 F.2d 820 (D.C. Cir. 1973), *cert denied*, 415 U.S. 977 (1974). Additionally, pursuant to law, any reasonably segregable portion of a responsive record must be provided after redaction of any allegedly exempt material. 5 U.S.C. §552(b).

I request a waiver of all fees for this request under 5. U.S.C. § 552(a)(4)(A)(iii). Disclosure of the requested information to Freedom Watch is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in my commercial interest. The Islamic Republic of Iran's goal of obtaining nuclear weapons affects the safety of both Israel and the United States, thus putting American citizens at risk. Furthermore, the release of classified information by any particular individual within the executive branch, including the president, further endangers the American people and raises a spectre of corruption within the federal government that must be examined. Freedom Watch is engaged in the active dissemination of public information as is evident by our ongoing public interest legal work and continual fight against corruption within the United States government, and international cases, particularly with regard to Iran. Freedom Watch's website, freedomwatchusa.org serves as the primary means of disseminating that information, and is seen by millions of people annually. In addition, officials of Freedom Watch frequently appear on radio and television to disseminate important information to the public.

Furthermore, on behalf of Freedom Watch I am requesting expedited handling as provided in 32 C.F.R. 286.4(d) because there is an urgency to inform the public about an actual or alleged federal government activity. Iran is reportedly on the verge of acquiring nuclear weapons and Israel is reportedly on the verge of attacking it to

Defense Department

FOIA Request

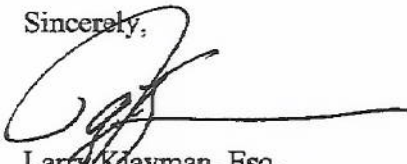
Page | 3

prevent their acquisition. The issue of Israel and a possible attack on Iran are of importance to the American people because Israel is an ally to the United States and any attack or war they declare will likely bring the United States into war as well. This fact is also evidenced in the articles mention above. Thus there is an immediate clear and present danger to U.S. citizens, American military personnel, American oil interests and the cost of gasoline and heating oil, which will likely skyrocket if Israel and Iran get engaged in war. This war can break out any time because a strike is needed before Iran can gain the capability to build a bomb. Thus, the well being of the American people is at immediate risk and they deserve to know on an expedited basis what their government is doing to try to protect them. And, importantly, the above mentioned "leaked" information is no longer in effect classified, as it was intentionally disclosed to the public, however illegally on orders by or on behalf of the President of the United States for political purposes, in any event.

The above mentioned "leaked" information is no longer in effect classified, if it ever was, as it was disclosed to the public by Mr. Sanger and The New York Times with the aid and complicity of President Obama and his administration. It was disclosed for political purposes to further President Obama's 2012 re-election campaign.

On behalf of Freedom Watch, I look forward to receiving the requested documents and a full fee waiver within ten (10) business days. You may have them delivered to the above address.

Sincerely,



Larry Klayman, Esq.
Chairman and General Counsel
2020 Pennsylvania Ave, N.W., Suite 345
Washington, D.C. 20006
leklayman@gmail.com

The New York Times

June 1, 2012

Obama Order Sped Up Wave of Cyberattacks Against Iran

By DAVID E. SANGER

WASHINGTON — From his first months in office, President Obama secretly ordered increasingly sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, significantly expanding America's first sustained use of cyberweapons, according to participants in the program.

Mr. Obama decided to accelerate the attacks — begun in the Bush administration and code-named Olympic Games — even after an element of the program accidentally became public in the summer of 2010 because of a programming error that allowed it to escape Iran's Natanz plant and sent it around the world on the Internet. Computer security experts who began studying the worm, which had been developed by the United States and Israel, gave it a name: Stuxnet.

At a tense meeting in the White House Situation Room within days of the worm's "escape," Mr. Obama, Vice President Joseph R. Biden Jr. and the director of the Central Intelligence Agency at the time, Leon E. Panetta, considered whether America's most ambitious attempt to slow the progress of Iran's nuclear efforts had been fatally compromised.

"Should we shut this thing down?" Mr. Obama asked, according to members of the president's national security team who were in the room.

Told it was unclear how much the Iranians knew about the code, and offered evidence that it was still causing havoc, Mr. Obama decided that the cyberattacks should proceed. In the following weeks, the Natanz plant was hit by a newer version of the computer worm, and then another after that. The last of that series of attacks, a few weeks after Stuxnet was detected around the world, temporarily took out nearly 1,000 of the 5,000 centrifuges Iran had spinning at the time to purify uranium.

This account of the American and Israeli effort to undermine the Iranian nuclear program is based on interviews over the past 18 months with current and former American, European and Israeli officials involved in the program, as well as a range of outside experts. None would allow

their names to be used because the effort remains highly classified, and parts of it continue to this day.

These officials gave differing assessments of how successful the sabotage program was in slowing Iran's progress toward developing the ability to build nuclear weapons. Internal Obama administration estimates say the effort was set back by 18 months to two years, but some experts inside and outside the government are more skeptical, noting that Iran's enrichment levels have steadily recovered, giving the country enough fuel today for five or more weapons, with additional enrichment.

Whether Iran is still trying to design and build a weapon is in dispute. The most recent United States intelligence estimate concludes that Iran suspended major parts of its weaponization effort after 2003, though there is evidence that some remnants of it continue.

Iran initially denied that its enrichment facilities had been hit by Stuxnet, then said it had found the worm and contained it. Last year, the nation announced that it had begun its own military cyberunit, and Brig. Gen. Gholamreza Jalali, the head of Iran's Passive Defense Organization, said that the Iranian military was prepared "to fight our enemies" in "cyberspace and Internet warfare." But there has been scant evidence that it has begun to strike back.

The United States government only recently acknowledged developing cyberweapons, and it has never admitted using them. There have been reports of one-time attacks against personal computers used by members of Al Qaeda, and of contemplated attacks against the computers that run air defense systems, including during the NATO-led air attack on Libya last year. But Olympic Games was of an entirely different type and sophistication.

It appears to be the first time the United States has repeatedly used cyberweapons to cripple another country's infrastructure, achieving, with computer code, what until then could be accomplished only by bombing a country or sending in agents to plant explosives. The code itself is 50 times as big as the typical computer worm, Carey Nachenberg, a vice president of Symantec, one of the many groups that have dissected the code, said at a symposium at Stanford University in April. Those forensic investigations into the inner workings of the code, while picking apart how it worked, came to no conclusions about who was responsible.

A similar process is now under way to figure out the origins of another cyberweapon called Flame that was recently discovered to have attacked the computers of Iranian officials, sweeping up information from those machines. But the computer code appears to be at least five years old, and American officials say that it was not part of Olympic Games. They have declined to say whether the United States was responsible for the Flame attack.

Mr. Obama, according to participants in the many Situation Room meetings on Olympic Games, was acutely aware that with every attack he was pushing the United States into new territory, much as his predecessors had with the first use of atomic weapons in the 1940s, of intercontinental missiles in the 1950s and of drones in the past decade. He repeatedly expressed concerns that any American acknowledgment that it was using cyberweapons — even under the most careful and limited circumstances — could enable other countries, terrorists or hackers to justify their own attacks.

“We discussed the irony, more than once,” one of his aides said. Another said that the administration was resistant to developing a “grand theory for a weapon whose possibilities they were still discovering.” Yet Mr. Obama concluded that when it came to stopping Iran, the United States had no other choice.

If Olympic Games failed, he told aides, there would be no time for sanctions and diplomacy with Iran to work. Israel could carry out a conventional military attack, prompting a conflict that could spread throughout the region.

A Bush Initiative

The impetus for Olympic Games dates from 2006, when President George W. Bush saw few good options in dealing with Iran. At the time, America’s European allies were divided about the cost that imposing sanctions on Iran would have on their own economies. Having falsely accused Saddam Hussein of reconstituting his nuclear program in Iraq, Mr. Bush had little credibility in publicly discussing another nation’s nuclear ambitions. The Iranians seemed to sense his vulnerability, and, frustrated by negotiations, they resumed enriching uranium at an underground site at Natanz, one whose existence had been exposed just three years before.

Iran’s president, Mahmoud Ahmadinejad, took reporters on a tour of the plant and described grand ambitions to install upward of 50,000 centrifuges. For a country with only one nuclear power reactor — whose fuel comes from Russia — to say that it needed fuel for its civilian nuclear program seemed dubious to Bush administration officials. They feared that the fuel could be used in another way besides providing power: to create a stockpile that could later be enriched to bomb-grade material if the Iranians made a political decision to do so.

Hawks in the Bush administration like Vice President Dick Cheney urged Mr. Bush to consider a military strike against the Iranian nuclear facilities before they could produce fuel suitable for a weapon. Several times, the administration reviewed military options and concluded that they would only further inflame a region already at war, and would have uncertain results.

For years the C.I.A. had introduced faulty parts and designs into Iran’s systems — even

tinkering with imported power supplies so that they would blow up — but the sabotage had had relatively little effect. General James E. Cartwright, who had established a small cyberoperation inside the United States Strategic Command, which is responsible for many of America’s nuclear forces, joined intelligence officials in presenting a radical new idea to Mr. Bush and his national security team. It involved a far more sophisticated cyberweapon than the United States had designed before.

The goal was to gain access to the Natanz plant’s industrial computer controls. That required leaping the electronic moat that cut the Natanz plant off from the Internet — called the air gap, because it physically separates the facility from the outside world. The computer code would invade the specialized computers that command the centrifuges.

The first stage in the effort was to develop a bit of computer code called a beacon that could be inserted into the computers, which were made by the German company Siemens and an Iranian manufacturer, to map their operations. The idea was to draw the equivalent of an electrical blueprint of the Natanz plant, to understand how the computers control the giant silvery centrifuges that spin at tremendous speeds. The connections were complex, and unless every circuit was understood, efforts to seize control of the centrifuges could fail.

Eventually the beacon would have to “phone home” — literally send a message back to the headquarters of the National Security Agency that would describe the structure and daily rhythms of the enrichment plant. Expectations for the plan were low; one participant said the goal was simply to “throw a little sand in the gears” and buy some time. Mr. Bush was skeptical, but lacking other options, he authorized the effort.

Breakthrough, Aided by Israel

It took months for the beacons to do their work and report home, complete with maps of the electronic directories of the controllers and what amounted to blueprints of how they were connected to the centrifuges deep underground.

Then the N.S.A. and a secret Israeli unit respected by American intelligence of cyberskills set to work developing the enormously complex computer worm that the attacker from within.

OPEN	MORE IN MI
	Egypt A Verdict
	Read More

The unusually tight collaboration with Israel was driven by two imperatives. I, a part of its military, had technical expertise that rivaled the N.S.A.’s, and the Israelis had deep intelligence about operations at Natanz that would be vital to making the cyberattack a success. But American officials had another interest, to dissuade the Israelis from carrying out their own pre-emptive strike against the Iranian nuclear facilities. To do that, the Israelis would have to

be convinced that the new line of attack was working. The only way to convince them, several officials said in interviews, was to have them deeply involved in every aspect of the program.

Soon the two countries had developed a complex worm that the Americans called “the bug.” But the bug needed to be tested. So, under enormous secrecy, the United States began building replicas of Iran’s P-1 centrifuges, an aging, unreliable design that Iran purchased from Abdul Qadeer Khan, the Pakistani nuclear chief who had begun selling fuel-making technology on the black market. Fortunately for the United States, it already owned some P-1s, thanks to the Libyan dictator, Col. Muammar el-Qaddafi.

When Colonel Qaddafi gave up his nuclear weapons program in 2003, he turned over the centrifuges he had bought from the Pakistani nuclear ring, and they were placed in storage at a weapons laboratory in Tennessee. The military and intelligence officials overseeing Olympic Games borrowed some for what they termed “destructive testing,” essentially building a virtual replica of Natanz, but spreading the test over several of the Energy Department’s national laboratories to keep even the most trusted nuclear workers from figuring out what was afoot.

Those first small-scale tests were surprisingly successful: the bug invaded the computers, lurking for days or weeks, before sending instructions to speed them up or slow them down so suddenly that their delicate parts, spinning at supersonic speeds, self-destructed. After several false starts, it worked. One day, toward the end of Mr. Bush’s term, the rubble of a centrifuge was spread out on the conference table in the Situation Room, proof of the potential power of a cyberweapon. The worm was declared ready to test against the real target: Iran’s underground enrichment plant.

“Previous cyberattacks had effects limited to other computers,” Michael V. Hayden, the former chief of the C.I.A., said, declining to describe what he knew of these attacks when he was in office. “This is the first attack of a major nature in which a cyberattack was used to effect physical destruction,” rather than just slow another computer, or hack into it to steal data.

“Somebody crossed the Rubicon,” he said.

Getting the worm into Natanz, however, was no easy trick. The United States and Israel would have to rely on engineers, maintenance workers and others — both spies and unwitting accomplices — with physical access to the plant. “That was our holy grail,” one of the architects of the plan said. “It turns out there is always an idiot around who doesn’t think much about the thumb drive in their hand.”

In fact, thumb drives turned out to be critical in spreading the first variants of the computer worm; later, more sophisticated methods were developed to deliver the malicious code.

The first attacks were small, and when the centrifuges began spinning out of control in 2008, the Iranians were mystified about the cause, according to intercepts that the United States later picked up. “The thinking was that the Iranians would blame bad parts, or bad engineering, or just incompetence,” one of the architects of the early attack said.

The Iranians were confused partly because no two attacks were exactly alike. Moreover, the code would lurk inside the plant for weeks, recording normal operations; when it attacked, it sent signals to the Natanz control room indicating that everything downstairs was operating normally. “This may have been the most brilliant part of the code,” one American official said.

Later, word circulated through the International Atomic Energy Agency, the Vienna-based nuclear watchdog, that the Iranians had grown so distrustful of their own instruments that they had assigned people to sit in the plant and radio back what they saw.

“The intent was that the failures should make them feel they were stupid, which is what happened,” the participant in the attacks said. When a few centrifuges failed, the Iranians would close down whole “stands” that linked 164 machines, looking for signs of sabotage in all of them. “They overreacted,” one official said. “We soon discovered they fired people.”

Imagery recovered by nuclear inspectors from cameras at Natanz — which the nuclear agency uses to keep track of what happens between visits — showed the results. There was some evidence of wreckage, but it was clear that the Iranians had also carted away centrifuges that had previously appeared to be working well.

But by the time Mr. Bush left office, no wholesale destruction had been accomplished. Meeting with Mr. Obama in the White House days before his inauguration, Mr. Bush urged him to preserve two classified programs, Olympic Games and the drone program in Pakistan. Mr. Obama took Mr. Bush’s advice.

The Stuxnet Surprise

Mr. Obama came to office with an interest in cyberissues, but he had discussed them during the campaign mostly in terms of threats to personal privacy and the risks to infrastructure like the electrical grid and the air traffic control system. He commissioned a major study on how to improve America’s defenses and announced it with great fanfare in the East Room.

What he did not say then was that he was also learning the arts of cyberwar. The architects of Olympic Games would meet him in the Situation Room, often with what they called the “horse blanket,” a giant foldout schematic diagram of Iran’s nuclear production facilities. Mr. Obama authorized the attacks to continue, and every few weeks — certainly after a major attack — he

would get updates and authorize the next step. Sometimes it was a strike riskier and bolder than what had been tried previously.

“From his first days in office, he was deep into every step in slowing the Iranian program — the diplomacy, the sanctions, every major decision,” a senior administration official said. “And it’s safe to say that whatever other activity might have been under way was no exception to that rule.”

But the good luck did not last. In the summer of 2010, shortly after a new variant of the worm had been sent into Natanz, it became clear that the worm, which was never supposed to leave the Natanz machines, had broken free, like a zoo animal that found the keys to the cage. It fell to Mr. Panetta and two other crucial players in Olympic Games — General Cartwright, the vice chairman of the Joint Chiefs of Staff, and Michael J. Morell, the deputy director of the C.I.A. — to break the news to Mr. Obama and Mr. Biden.

An error in the code, they said, had led it to spread to an engineer’s computer when it was hooked up to the centrifuges. When the engineer left Natanz and connected the computer to the Internet, the American- and Israeli-made bug failed to recognize that its environment had changed. It began replicating itself all around the world. Suddenly, the code was exposed, though its intent would not be clear, at least to ordinary computer users.

“We think there was a modification done by the Israelis,” one of the briefers told the president, “and we don’t know if we were part of that activity.”

Mr. Obama, according to officials in the room, asked a series of questions, fearful that the code could do damage outside the plant. The answers came back in hedged terms. Mr. Biden fumed. “It’s got to be the Israelis,” he said. “They went too far.”

In fact, both the Israelis and the Americans had been aiming for a particular part of the centrifuge plant, a critical area whose loss, they had concluded, would set the Iranians back considerably. It is unclear who introduced the programming error.

The question facing Mr. Obama was whether the rest of Olympic Games was in jeopardy, now that a variant of the bug was replicating itself “in the wild,” where computer security experts can dissect it and figure out its purpose.

“I don’t think we have enough information,” Mr. Obama told the group that day, according to the officials. But in the meantime, he ordered that the cyberattacks continue. They were his best hope of disrupting the Iranian nuclear program unless economic sanctions began to bite harder and reduced Iran’s oil revenues.

Within a week, another version of the bug brought down just under 1,000 centrifuges. Olympic Games was still on.

A Weapon's Uncertain Future

American cyberattacks are not limited to Iran, but the focus of attention, as one administration official put it, "has been overwhelmingly on one country." There is no reason to believe that will remain the case for long. Some officials question why the same techniques have not been used more aggressively against North Korea. Others see chances to disrupt Chinese military plans, forces in Syria on the way to suppress the uprising there, and Qaeda operations around the world. "We've considered a lot more attacks than we have gone ahead with," one former intelligence official said.

Mr. Obama has repeatedly told his aides that there are risks to using — and particularly to overusing — the weapon. In fact, no country's infrastructure is more dependent on computer systems, and thus more vulnerable to attack, than that of the United States. It is only a matter of time, most experts believe, before it becomes the target of the same kind of weapon that the Americans have used, secretly, against Iran.

This article is adapted from "Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power," to be published by Crown on Tuesday.

12-F-0966



FREEDOM WATCH

www.FreedomWatchUSA.org

World Headquarters 2020 Pennsylvania Avenue, N.W., Suite 345, Washington, DC 20036-1811 (310) 595-0800 1ckleyman@gmail.com

FAX

To: Department of Defense **From:** Freedom Watch

Fax: 571-372-0500 **Pages:** 11 (excluding this one)

Phone: **Date:** 06-01-12

Re: FOIA Request **CC:**

Urgent For Review Please Comment Please Reply

ATTACHMENT 2



DEPARTMENT OF DEFENSE
OFFICE OF FREEDOM OF INFORMATION
1155 DEFENSE PENTAGON
WASHINGTON, DC 20301-1155

07 JUN 2012

Ref: 12-F-0966

Mr. Larry Klayman
Freedom Watch
2020 Pennsylvania Ave., NW
STE 345
Washington, D.C. 20006

Dear Mr. Klayman:

This letter acknowledges the receipt of your June 1, 2012, Freedom of Information Act (FOIA) request for information leaked pertaining to cyberattacks against Iran. We received your request on June 1, 2012 and noted your request for expedited treatment.

Regarding your request for expedited processing, you are asking this Office to place your request ahead of all other requests received. This Office, however, receives hundreds of FOIA requests. According to DoD Regulation 5400.7-R, in order to qualify for expedited processing, a requester must demonstrate a "compelling need" for the information, i.e., that failure to obtain the records on an expedited basis reasonably could be expected to pose an imminent threat to the life or physical safety of an individual, or an imminent loss of substantial due process rights, or humanitarian need.

Expedited processing may be granted when the requester demonstrates a compelling need for the information and shows that the information has a particular value that would be lost if not processed on an expedited basis. A key word here is "demonstrates." It is, therefore, incumbent upon you to demonstrate that the requested records will serve an urgency purpose, and that they also will be meaningful in the sense that they will provide for a greater understanding of actual or alleged federal government activity on the part of the public-at-large than that which existed before such information was disseminated. Consequently, it must be clearly demonstrated that such information has a particular value that will be lost if not disseminated quickly. After careful consideration of your request, this Office finds that you have not clearly demonstrated how the information will lose its value if not processed on an expedited basis. For these reasons, your request for expedited processing is denied.

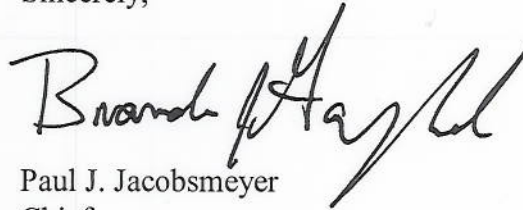
With regard to your request for a waiver of any applicable fees, a fee waiver is appropriate when "disclosure of the requested information is in the public interest because it is likely to contribute significantly to public understanding of the operations and activities of the government and is not primarily in the commercial interest of the requester." 5 U.S.C. § 552(a)(4)(iii). Decisions to waive or reduce fees are made on a case-by-case basis. I will consider your request for a fee waiver after a search is completed and this Office determines if records responsive to your request exist, and the volume and nature of those records.

JA109

You should also know that we will be unable to respond to your request within the FOIA's 20 day statutory time period as there are unusual circumstances which impact on our ability to quickly process your request. These unusual circumstances are: (a) the need to search for and collect records from a facility geographically separated from this Office; (b) the potential volume of records responsive to your request; and (c) the need for consultation with one or more other agencies or DoD components having a substantial interest in either the determination or the subject matter of the records. For these reasons, your request has been placed in our complex processing queue and will be worked in the order the request was received. Our current administrative workload is 1,260 open requests. If you have any questions regarding this action please contact Brandon Gaylord at brandon.gaylord@whs.mil or (571) 372-0413.

If you are not satisfied with this action, you may appeal to the appellate authority, the Director of Administration and Management, Office of the Secretary of Defense, by writing directly to the Defense Freedom of Information Policy Office, Attn: Mr. James Hogan, 1155 Defense Pentagon, Washington, D.C. 20301-1155. Your appeal should be postmarked within 60 calendar days of the date of this letter, should cite to case number 12-F-0966, and should be clearly marked "Freedom of Information Act Appeal."

Sincerely,



for

Paul J. Jacobsmeyer
Chief

ATTACHMENT 3



DEPARTMENT OF DEFENSE
DEFENSE FREEDOM OF INFORMATION POLICY OFFICE
1155 DEFENSE PENTAGON
WASHINGTON, DC 20301-1155

October 1, 2012
Ref: 12-L-0966

Mr. Larry Klayman
Freedom Watch
2020 Pennsylvania Ave., NW
STE 345
Washington, D.C. 20006

Dear Mr. Klayman:

This is the final response to your Freedom of Information Act request dated June 1, 2012, for documents related to information leaked pertaining to cyber attacks against Iran. We received your request on the same day that it was submitted.

The Joint Staff has determined that the fact of the existence or nonexistence of documents concerning the matters relating to those set forth in your request is classified in accordance with Executive Order 13526. Therefore, pursuant to 5 USC 552 (b)(1), Mr. Mark S. Patrick, Chief, Information Management Division, Joint Staff has denied your request. By this statement, the Department of Defense neither confirms nor denies that such documents may or may not exist.

Since this is a matter of litigation your appellate rights are moot.

Sincerely,

A handwritten signature in black ink that reads "James P. Hogan".

James P. Hogan
Chief

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

FREEDOM WATCH, INC.,

Plaintiff,

v.

NATIONAL SECURITY AGENCY;
CENTRAL INTELLIGENCE AGENCY;
DEPARTMENT OF DEFENSE; and
DEPARTMENT OF STATE,

Defendants.

Case No. 1:12-cv-01088
Judge Robert L. Wilkins

ORDER

Upon consideration of Defendants' Motion for Judgment on the Pleadings and Motion for Partial Summary Judgment, and for the reasons stated on the record in open court on December 10, 2012, it is hereby

ORDERED that the Motion for Judgment on the Pleadings of Defendants National Security Agency and Central Intelligence Agency is GRANTED; and it is

FURTHER ORDERED that Defendant Department of Defense's Motion for Partial Summary Judgment is GRANTED; and it is

FURTHER ORDERED that Defendant Department of State's Motion for Judgment on the Pleadings is GRANTED with respect to Request Numbers 1 and 3-6 of Plaintiff's Freedom of Information Act request; and it is

FURTHER ORDERED that Defendant Department of State's Motion for Judgment on the Pleadings is DENIED with respect to Request Number 2.

Date: December 13, 2012



Digitally signed by Judge Robert L. Wilkins
DN: cn=Judge Robert L. Wilkins, o=U.S.
District Court, ou=Chambers of Honorable
Robert L. Wilkins,
email=RW@dc.uscourts.gov, c=US
Date: 2012.12.13 13:41:00 -05'00'

THE HONORABLE ROBERT L. WILKINS
UNITED STATES DISTRICT JUDGE

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

FREEDOM WATCH, INC.,

Plaintiff,

v.

NATIONAL SECURITY AGENCY;
CENTRAL INTELLIGENCE AGENCY;
DEPARTMENT OF DEFENSE; and
DEPARTMENT OF STATE,

Defendants.

Case No. 1:12-cv-01088
Judge Robert L. Wilkins

ORDER

Upon consideration of the parties' Joint Status Report (Dkt. No. 9), it is hereby ORDERED that no later than March 18, 2013, Defendant Department of State ("State") will: (1) conclude its search for records responsive to Plaintiff's Request Number 2 that relate to the June 1, 2012 *New York Times* article, (2) process and produce any non-exempt records; and (3) produce a *Vaughn* index (to the extent one is required); and it is

FURTHER ORDERED that State will then file a dispositive motion no later than April 17, 2013.

Date: December 18, 2012



Digitally signed by Judge Robert L. Wilkins
DN: cn=Judge Robert L. Wilkins, o=U.S. District
Court, ou=Chambers of Honorable Robert L.
Wilkins, email=RW@dc.uscourts.gov, c=US
Date: 2012.12.18 10:35:15 -05'00'

THE HONORABLE ROBERT L. WILKINS
UNITED STATES DISTRICT JUDGE

THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

FREEDOM WATCH, INC.,
Plaintiff,

v.

NATIONAL SECURITY AGENCY, *et*
al.,

Defendants.

§
§
§
§
§
§
§
§

No. 1:12-cv-01088

SUPPLEMENTAL DECLARATION OF SHERYL L. WALTER

Pursuant to 28 U.S.C. § 1746, I, Sheryl L. Walter, declare and state as follows:

1. I am the Director of the Office of Information Programs and Services (“IPS”) of the United States Department of State (the “Department”). In this capacity, I am the Department official immediately responsible for responding to requests for records under the Freedom of Information Act (the “FOIA”), 5 U.S.C. § 552, the Privacy Act of 1974, 5 U.S.C. § 552a, and other applicable records access provisions. I have been employed by the Department in this capacity since 2011. As IPS Director, I am authorized to classify and declassify national security information. I make the following statements based upon my personal knowledge, which in turn is based on a personal review of the records in the case file established for processing the subject request and upon information furnished to me in the course of my official duties.

2. The core responsibilities of IPS include: (1) responding to records access requests made by the public (including under the FOIA, the Privacy Act, the mandatory declassification review requirements of the Executive Order governing classified national security information, or the Ethics in Government Act), by members of Congress, by other government agencies, and

those made pursuant to judicial process such as subpoenas, court orders, and discovery requests; (2) records management; (3) privacy protection; (4) national security classification management and declassification review; (5) corporate records archives management; (6) research; (7) operation and management of the Department's library; and (8) technology applications that support these activities.

3. This declaration explains the Department's search for records responsive to the FOIA request at issue in this litigation.

I. ADMINISTRATIVE PROCESSING OF THE REQUEST

FOIA Case No. F-2012-28257

4. By letter dated June 1, 2012 (Exhibit 1), Freedom Watch ("Plaintiff") made a request under the FOIA for records that refer or relate to

- 1) Any and all information that refers or relates to the New York Times article entitled "Obama Order Sped Up Wave of Cyberattacks Against Iran" by David E. Sanger on Friday, June 1, 2012, and which information was provided and leaked to Mr. Sanger and the New York Times;
- 2) Any and all information that refers or relates in any way to information released to David E. Sanger and/or made available to him;
- 3) The names of the persons, employers and job titles, and addresses of those who "leaked" the above information to David E. Sanger;
- 4) Communications with The White House and/or Office of the President and/or Vice President that refer or relate in any way to the "leaked" information and/or the reasons for "leaking" the information;
- 5) Any and all information that refer or relate to the decision to "leak" the above previously classified information;
- 6) Any and all information that refers or relates to government agencies deciding to investigate who "leaked" the above previously classified information.

Plaintiff did not limit the timeframe of its request. Plaintiff requested a fee waiver, as well as expedited processing of his request.

5. By letter dated June 27, 2012 (Exhibit 2), IPS acknowledged receipt of Plaintiff's request and assigned it FOIA Case Control Number F-2012-28257. The letter notified Plaintiff that the processing of his request had begun and that he would be notified as soon as responsive material was retrieved and reviewed. The letter advised Plaintiff that the cut-off date for retrieving records was either the date he had given the Department or the date the search was initiated. The letter also advised Plaintiff that his request had not met the standard for expedited processing set forth in the Department's published regulations, and that a decision on his request for a fee waiver had been deferred. Finally, the Department advised Plaintiff of his right to appeal this decision.

6. On June 28, 2012, Plaintiff filed a complaint against the Department, the National Security Agency ("NSA"), the Central Intelligence Agency ("CIA"), and the Department of Defense ("DoD") in the United States District Court for the District of Columbia to compel compliance with the FOIA.

7. On December 13, 2012, the Court granted CIA and NSA's motion for judgment on the pleadings and DoD's motion for partial summary judgment, as well as the Department's motion for judgment on the pleadings with respect to items 1 and 3-6 of Plaintiff's June 2012 FOIA request. However, the Court denied the Department's motion with respect to item 2 of that request.

8. By letter dated March 18, 2013 (Exhibit 3), IPS notified Plaintiff that the Department had conducted searches of the following Department records systems: the Central Foreign Policy Records, the Bureau of Public Affairs, and the Bureau of Near Eastern Affairs.

IPS further advised Plaintiff that no responsive records had been located as a result of these searches and that the processing of his request had been completed.

9. After the issuance of the March 18 letter, and during the preparation of this declaration, the Bureau of Public Affairs revisited its searches and located three documents responsive to item 2 of Plaintiff's request. One of the documents, entitled "NSC Daily Press Guidance," originated with the National Security Staff (the "NSS"). As a result, the Department referred this document to the NSS for its review. The Department released all responsive material in the NSS document and all material in the other two documents to Plaintiff by letter dated April 17, 2013 (Exhibit 4).

II. THE SEARCH PROCESS

10. When the Department receives a FOIA request, IPS evaluates the request to determine which offices, overseas posts, or records systems within the Department may reasonably be expected to contain the records requested. This determination is based on the description of the records requested and requires a familiarity with the holdings of the Department's records systems, applicable records disposition schedules, and the substantive and functional mandates of numerous Department offices and Foreign Service posts and missions. Factors such as the nature, scope, and complexity of the request itself are also relevant.

11. Each office within the Department, as well as each Foreign Service post and mission, maintains files concerning foreign policy and other functional matters related to the daily operations of that office, post, or mission. These files consist generally of working copies of documents, informational copies of documents maintained in the Central Foreign Policy Records collection, and other documents prepared by or furnished to the office in connection

with the performance of its official duties, as well as electronic copies of documents and e-mail messages.

12. After reviewing Plaintiff's request, IPS determined that the offices or records systems with a reasonable possibility of possessing responsive documents were the Central Foreign Policy Records, the Bureau of Public Affairs, and the Bureau of Near Eastern Affairs. Individuals who were familiar with both the subject matter of Plaintiff's request and the content and organization of the records systems in these offices conducted the searches for responsive records.

The Central Foreign Policy Records

13. The records of the Department are maintained in both centralized and decentralized records systems. The Central Foreign Policy Records (or "Central File") is the Department's centralized records system and contains over 30 million records of a substantive nature that establish, discuss, or define foreign policy, set precedents, or require action or use by more than one office. Among other things, the Central File includes official record copies of almost all incoming and outgoing telegrams between the Department and Foreign Service posts, as well as other select substantive correspondence, including: diplomatic notes; correspondence to and from the White House, members of Congress, and other federal agencies; position papers and reports; memoranda of conversations; and interoffice memoranda. Because the Central File is the Department's most comprehensive and authoritative compilation of records, it is by far the records system most frequently searched in response to FOIA requests. Searches of the Central File are conducted through an automated interface, known as the State Archiving System ("SAS"), which searches the full text of millions of telegrams and other substantive correspondence in the Central File. For all documents in the Central File that are not directly

full-text searchable through SAS, including some older correspondence, SAS will search the text of a customized reference index that directs a searcher to a full copy of the document. Thus, a SAS search will encompass all documents in the Central File.

14. An IPS researcher with knowledge of both the request and the records system conducted a full-text search of the Central File using the following separate search terms: “David Sanger” and “David E. Sanger.” The search was structured to capture responsive records created between June 1, 2011 and February 12, 2013 (the date the search was conducted). This search located no responsive documents.

The Bureau of Public Affairs

15. The Bureau of Public Affairs (“PA”) engages domestic and international media to communicate timely and accurate information with the goals of furthering U.S. foreign policy and national security interests and broadening understanding of American values. In carrying out its mission, PA employs a wide range of media platforms, provides historical perspective, and conducts public outreach.

16. The PA Press Office engages with media on a daily basis, using Microsoft Outlook to transmit and record journalist queries. Journalists contact the office via a collective e-mail address or by calling a main telephone line. All calls are received by front desk staff, who e-mail the reporter’s name, contact information, and the subject of the inquiry to an office collective address. Press officers will pick up the calls and respond to journalists via e-mail or by phone. This is all done electronically; no paper records related to such contacts with journalists are maintained.

17. PA Press Office management asked all eight press officers, the Director, and the Deputy Director to review their records carefully for any calls or e-mails from David Sanger.

The employees searched all electronic records, including personal and collective e-mail accounts, shared drives, and personal electronic files using the following separate search terms: “David Sanger” and “David E. Sanger”. The searches were structured to capture responsive records created between June 1, 2011 and April 12, 2013 (the date the searches were conducted). PA located three responsive documents as a result of these searches.

The Bureau of Near Eastern Affairs

18. The Bureau of Near Eastern Affairs (“NEA”) is charged with advising the Secretary of State on matters in North Africa and the Middle East. Regional policy issues that NEA handles include Iran, Iraq, the Middle East peace process, terrorism and weapons of mass destruction, and political and economic reform.

19. Employees of NEA’s Iran Office were tasked to review their files for any reference to David Sanger in connection with alleged cyberattacks on Iran. One Office Director, one Deputy Director, six Desk Officers, four Foreign Affairs Officers, one Intern, one Senior Advisor for Strategic Communications, and one Public Affairs Officer searched their files for responsive records. The searches were structured to capture responsive records created between June 1, 2011 to December 28, 2012 (the date the searches were initiated). The aforementioned NEA employees searched electronic records and e-mails on shared drives and individual computers using the search term “David Sanger” on both OpenNet (the Department’s unclassified network) and ClassNet (the Department’s classified network). Additionally, the Iran Office maintains two office safes for classified paper documents, located in the Director’s and Deputy Director’s offices. The Iran Office determined that these safes were the only non-electronic locations with a reasonable possibility of containing information responsive to this FOIA request. NEA searched both safes, and the Director and Deputy Director certified that

neither safe contained material responsive to this request. NEA located no responsive documents as a result of these searches.

CONCLUSION

20. In summary, the Department conducted a thorough search of all components that it determined had a reasonable possibility of possessing records responsive to item 2 of Plaintiff's FOIA request and located three responsive records. The Department released all responsive material in full to Plaintiff.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Executed this 17th day of April 2013, Washington, D.C.

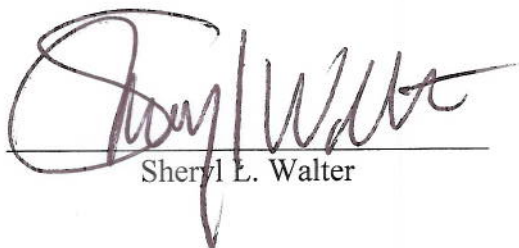

Sheryl E. Walter

EXHIBIT 3



United States Department of State

Washington, D.C. 20520

MAR 18 2013

Case No.: F-2012-28257

Mr. Larry Klayman, Esq.
Freedom Watch
2020 Pennsylvania Ave. NW, Suite 345
Washington, DC 20006

Dear Mr. Klayman:

I refer to your letter dated June 1, 2012 requesting under the provisions of the Freedom of Information Act (Title 5 USC Section 552) the release of certain records maintained by the Department of State.

The Department conducted thorough searches of the following records systems for records responsive to item 2 of your request: the Central Foreign Policy Records (the principal records system of the Department of State), the Bureau of Public Affairs, and the Bureau of Near Eastern Affairs. No records responsive to your request were located.

The processing of your request has now been completed. If you have any questions, you may contact John Theis, Assistant U.S. Attorney, at (202) 305-7632.

Sincerely,

A handwritten signature in cursive script that reads "Sheryl L. Walter" followed by a stylized set of initials.

Sheryl L. Walter, Director
Office of Information Programs and Services

EXHIBIT 4



Washington, D.C. 20520

APR 17 2013

Case No.: F-2012-28257

Mr. Larry Klayman, Esq.
Freedom Watch
2020 Pennsylvania Ave. NW, Suite 345
Washington, DC 20006

Dear Mr. Klayman:

I refer to our letter dated March 18, 2013 regarding the release of certain Department of State material under the Freedom of Information Act (Title 5 USC Section 552).

Following the issuance of the March 18 letter, the Bureau of Public Affairs revisited its searches and located three documents responsive to your request. One of the documents originated with another agency and was referred to that agency for its review. Upon review, the originating agency determined that most of the information in that document was not responsive to your request and redacted the non-responsive information accordingly. However, all responsive information in that document is being released to you. We determined that the other two documents may be released in full. All released material is enclosed.

The processing of your request has now been completed. If you have any questions, you may contact John Theis, Trial Attorney, U.S. Department of Justice, at (202) 305-7632.

Sincerely,

Sheryl L. Walter | SW

Sheryl L. Walter, Director
Office of Information Programs and Services

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

FREEDOM WATCH, INC.

Plaintiff,

v.

**NATIONAL SECURITY AGENCY, ET.
AL.,**

Defendants.

Civil Action No. 1:12-cv-01088-RLW

**FRCP RULE 56(d) AFFIDAVIT OF LARRY KLAYMAN IN SUPPORT OF
PLAINTIFF'S OPPOSITION TO DEFENDANTS' MOTION FOR SUMMARY
JUDGMENT**

Larry Klayman, Chairman and General Counsel of Plaintiff Freedom Watch, being duly sworn, hereby deposes and says:

1. Plaintiff requests discovery pursuant to Federal Rules of Civil Procedure ("FRCP") 56(d) concerning the claimed facts set forth in the declarations of Sheryl L. Walters, that Defendants have advanced as grounds for summary judgment.
2. Defendants are in sole possession of information necessary for determination of any such summary judgment proceeding, including but not limited to:
 - a) the identity of the custodian of records at the "originating agency" of one of the documents produced by defendants as referred to by Sheryl L. Walters;
 - b) the description of the records redacted and marked "non-responsive";
 - c) the details regarding the review of documents by "originating agency" and the determination that certain documents were non-responsive and thus, not produced; and

- d) the full record, including but not limited to, and notes, writings, and/or electronic recordings from the interview between David E. Sanger and Secretary of State Hillary Clinton.
3. Without discovery concerning the documents and other materials requested in paragraph 2 of Plaintiff's FOIA request, Plaintiff is unable to justify its opposition to Defendant's Motion for Summary Judgment. This is more fully set forth in Plaintiff's Opposition To Defendant's Motion For Summary Judgment which is incorporated into this affidavit by reference.
4. Plaintiff requires discovery in the form of depositions of the custodians of records for the involved agencies, including, but not limited to, Sheryl L. Walters, a review of relevant documents and information that are in sole custody of the Defendant, and such other discovery as required to ascertain the facts relevant to Defendants' court-ordered Motion for Summary Judgment.

Dated: May 20, 2013

/s/ Larry Klayman
Larry Klayman
Chairman and General Counsel
Freedom Watch, Inc.

THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

FREEDOM WATCH, INC.,	§	
Plaintiff,	§	
	§	
v.	§	
	§	No. 1:12-cv-01088
NATIONAL SECURITY AGENCY <i>et</i>	§	
<i>al.</i> ,	§	
	§	
Defendants.	§	

SECOND SUPPLEMENTAL DECLARATION OF SHERYL L. WALTER

Pursuant to 28 U.S.C. § 1746, I, Sheryl L. Walter, declare and state as follows:

1. I am the Director of the Office of Information Programs and Services (“IPS”) of the United States Department of State (the “Department”). In this capacity, I am the Department official immediately responsible for responding to requests for records under the Freedom of Information Act (the “FOIA”), 5 U.S.C. § 552, the Privacy Act of 1974, 5 U.S.C. § 552a, and other applicable records access provisions. I have been employed by the Department in this capacity since 2011. I am the same Sheryl Walter who executed declarations in this case on October 4, 2012 and April 17, 2013. As IPS Director, I am authorized to classify and declassify national security information. I make the following statements based upon my personal knowledge, which in turn is based on a personal review of the records in the case file established for processing the subject request and upon information furnished to me in the course of my official duties. I am familiar with the efforts of Department personnel to process the subject request, and I am in charge of coordinating the agency’s search and recovery efforts with respect to that request.

2. The core responsibilities of IPS include: (1) responding to records access requests made by the public (including under the FOIA, the Privacy Act, the mandatory declassification review requirements of the Executive Order governing classified national security information, or the Ethics in Government Act), by members of Congress, by other government agencies, and those made pursuant to judicial process such as subpoenas, court orders, and discovery requests; (2) records management; (3) privacy protection; (4) national security classification management and declassification review; (5) corporate records archives management; (6) research; (7) operation and management of the Department's library; and (8) technology applications that support these activities. The purposes of this declaration are to respond to Plaintiff's opposition to the Department's motion for summary judgment, describe the details of the Department's supplemental search for records, and describe the redactions made to responsive records prior to production.

I. THE REDACTION OF NON-RESPONSIVE NATIONAL SECURITY STAFF MATERIAL

3. As stated previously, IPS notified Plaintiff that the Bureau of Public Affairs located three documents responsive to item 2 of Plaintiff's request. One of the documents (P1), entitled "NSC Daily Press Guidance," originated with the National Security Staff (the "NSS"). See Supplemental Walter Declaration dated April 17, 2013, at ¶ 9. After consulting with the NSS, the Department released all responsive material in the NSS document and all material in the other two documents to Plaintiff by letter dated April 17, 2013.

4. As the title of the NSS document indicates, it contains guidance on a number of different issues that were of current media interest on June 1, 2012. Only one of these issues was responsive to Plaintiff's targeted request for "any and all information that refers or relates in any

way to information released to David E. Sanger and/or made available to him” (item 2 of Plaintiff’s FOIA request). For this reason, at the request of the NSS, the Department redacted the non-responsive NSS information and released the responsive information contained in the document.

II. THE DEPARTMENT’S SUPPLEMENTAL SEARCHES

A. The Bureau of Public Affairs

5. As explained in my declaration dated April 17, 2013, the Bureau of Public Affairs (“PA”) engages domestic and international media to communicate timely and accurate information with the goals of furthering U.S. foreign policy and national security interests and broadening understanding of American values. In carrying out its mission, PA employs a wide range of media platforms, provides historical perspective, and conducts public outreach.

6. After carefully reviewing Plaintiff’s opposition to the Department’s motion for summary judgment, the Department asked PA to confirm that no other locations within the Bureau should be searched in response to Plaintiff’s FOIA request in addition to PA’s Press Office, the search of which was described in paragraph 17 of my April 17 declaration. In response, PA explained that it had inadvertently failed to task the PA Front Office (“PA/FO”), which performs executive functions in support of the bureau’s mission, in its original response to the subject request, and it immediately initiated a supplemental search of PA/FO for records responsive to item 2 of Plaintiff’s request.

7. In this supplemental search, all 17 PA/FO employees, including the Assistant Secretary of State for Public Affairs, searched their paper and electronic files for records responsive to Plaintiff’s request using the timeframe of June 1, 2011 through April 12, 2013 (the date on which PA initiated its search for records responsive to Plaintiff’s request). The PA/FO

employees searched their electronic files using the search terms “Sanger” and “David Sanger” and their hard-copy files by manually paging through paper records in their inboxes, drawers, and desktops for any records related to David Sanger. PA/FO primarily maintains electronic files unless they need to print a document for short-term use before recycling it. Additionally, information technology personnel conducted an electronic search using the term “Sanger” of the archived e-mail of three employees no longer in PA/FO who were identified as potential custodians of responsive records.

8. A review of the records retrieved in the PA/FO search indicated that David Sanger interviewed the following individuals for purposes of writing the book from which he derived, at least in part, his June 1, 2012 *New York Times* article: William Burns, Deputy Secretary of State; Robert Einhorn, then-Special Advisor for Nonproliferation and Arms Control; Harold Koh, then-Legal Adviser; Wendy Sherman, Under Secretary of State for Political Affairs; and Jake Sullivan, then-Director of the Department’s Policy Planning Staff. By virtue of these individuals’ positions and/or responsibilities, and absent information in the records indicating that these individuals did *not* discuss any of the subjects of the June 1, 2012 article, the Department could not rule out the possibility—however remote it might be—that their interviews with Mr. Sanger may have covered certain of the material discussed in his article. Thus, in an abundance of caution, the Department considered Mr. Sanger’s interviews with these individuals to be within the scope of Plaintiff’s request. In light of this development, the Department tasked the offices in which these individuals work (or worked at the relevant time) to search for records responsive to Plaintiff’s request. Details of these searches are provided below.

9. As a result of its supplemental searches, PA located 62 responsive records. By letter dated July 30, 2013, the Department released 43 documents in full and 18 documents in part to Plaintiff and withheld one document in full.

B. The Policy Planning Staff

10. In response to the Department's tasking, the Policy Planning Staff ("S/P") conducted a search of its shared drive using the term "Sanger." Jake Sullivan, the former director of S/P, is no longer employed by the Department; as a result, S/P does not possess any of Mr. Sullivan's paper and electronic records, which had been retired according to Department procedure. In order to search Mr. Sullivan's records, the Department's Executive Secretariat retrieved his still-existing e-mail accounts and performed a search using the search terms "Sanger" and "David Sanger," with a date range of June 1, 2011 to June 13, 2013 (the date the search was performed). Additionally, IPS retrieved Mr. Sullivan's retired paper files and manually searched those records for responsive documents.

11. S/P located four responsive records as a result of this search. By letter dated July 30, 2013, the Department released four documents in full to Plaintiff.

C. The Office of the Legal Adviser

12. The Office of the Legal Adviser ("L") conducted a search using the term "Sanger" of its electronic records management systems and the e-mail of L employees, including Harold Koh, who had a reasonable possibility of possessing potentially responsive records. This search was structured to capture responsive records created between June 1, 2011 and July 11, 2013 (the date the search was conducted). L also searched paper records, including correspondence and chronological files of the Legal Adviser in the L Front Office for any records related to David Sanger.

13. L located three responsive records as a result of this search. By letter dated July 30, 2013, the Department released three documents in full to Plaintiff.

D. The Office of Deputy Secretary of State William Burns

14. The Office of Deputy Secretary of State William Burns conducted an electronic search of Mr. Burns's e-mail, as well as of the electronic records system (known as "Everest") used to transmit memoranda to the Department's leadership, including Mr. Burns, using the search term "Sanger" for the time frame June 1, 2011 to June 13, 2013 (the date the search was performed). Additionally, the Office of the Deputy Secretary searched the paper records files containing the Deputy Secretary's memoranda, which are organized chronologically, for any records related to David Sanger.

15. The Office of the Deputy Secretary located two responsive records as a result of this search. By letter dated July 30, 2013, the Department released one document in full and one document in part to Plaintiff.

E. The Office of the Under Secretary of State for Political Affairs

16. The Office of the Under Secretary of State for Political Affairs ("P") conducted a search using the term "Sanger" of the electronic records, including e-mails, from June 1, 2011 to June 19, 2013 (the date the search was performed). P searched the paper and electronic files of the Under Secretary of State for Political Affairs (Wendy Sherman), an Executive Assistant, seven Special Assistants, and one Scheduler. The paper files are individually maintained in personal filing cabinets, where meeting requests are organized in files by the last name of the person requesting the meeting. P also searched shared drives, personal electronic files, and a file-sharing intranet site using the search term "Sanger."

17. P located three responsive records as a result of this search. By letter dated July 30, 2013, the Department released two documents in full and one document in part to Plaintiff.

F. The Office of the Special Advisor for Nonproliferation and Arms Control

18. The Office of the Special Advisor for Nonproliferation and Arms Control (“S/SANAC”) was disbanded in May 2013. Mr. Einhorn’s former assistant conducted a search using the term “Sanger” of the electronic records, including e-mails and calendar entries belonging to the assistant, as well as a search of all of Mr. Einhorn’s paper records, which were being reviewed in preparation for retirement. The former assistant also searched the shared directories for S/SANAC documents such as memoranda and letters. In order to search Mr. Einhorn’s electronic records, the Department’s Executive Secretariat retrieved his still-existing e-mail accounts and performed a search using the search terms “Sanger” and “David Sanger,” with a date range of June 1, 2011 to June 13, 2013 (the date the search was performed.)

19. S/SANAC located two responsive records as a result of this search. By letter dated July 30, 2013, the Department released both documents in full to Plaintiff.

III. EXEMPTIONS CLAIMED

FOIA Exemption (b)(5) – Privileged Information

20. Title 5 U.S.C. § 552(b)(5) states that the FOIA does not apply to inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency

21. Exemption (b)(5) protects from disclosure information that is normally privileged in the civil discovery context, including information that is protected by the deliberative process privilege.

22. The deliberative process privilege protects the candid views and advice of U.S. Government officials in their pre-decisional deliberations related to policy formulation and administrative direction. Disclosure of material containing such deliberations or material on which such deliberations are based would prejudice the free flow of internal recommendations and other necessary exchanges and would severely hamper the ability of responsible officials to formulate and carry out executive branch programs. The Department withheld information in four documents described in this *Vaughn* index—specifically, documents C05404110, C05404362, C05389507, and C05406079 discussed in more detail below—on the basis of Exemption (b)(5) and the deliberative process privilege. Disclosure of this information—which is inter- or intra-agency, pre-decisional, and deliberative, and contains selected factual material intertwined with opinion—would inhibit candid internal discussion and the expression of recommendations and judgments regarding the formulation of a strategy for the Department’s response to a matter that was urgent and developing at the time the documents were created, as well as options and recommendations regarding the preferred course of action. Additionally, in the case of deliberative drafts, release could result in public confusion as to the actual U.S. policy ultimately adopted on the issues discussed therein. With respect to the information withheld under Exemption (b)(5) pursuant to the deliberative process privilege, the Department has determined that there are no reasonably segregable facts that are not inextricably connected to the deliberative material that may be released. The withheld information is, accordingly, exempt from release under FOIA Exemption (b)(5), 5 U.S.C. § 552(b)(5).

FOIA Exemption (b)(6) – Personal Privacy

23. Title 5 U.S.C. § 552(b)(6) states that the FOIA does not apply to

personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy

24. Courts have interpreted the language of FOIA Exemption (b)(6) broadly to encompass all information that applies to an individual without regard to whether it was located in a particular type of file. The Department has withheld personal information regarding private individuals and certain government personnel in 17 documents addressed in this *Vaughn* index—specifically, documents C05404370, C05404222, C05404149, C05404369, C05404325, C05404185, C05404152, C05404373, C05404372, C05404139, C05904092, C05404181, C05404197, C05404351, C05404358, C05404364, and C05404366 discussed in more detail below—because the release of this information would constitute a clearly unwarranted invasion of personal privacy because it could result in harassment and unwanted attention.

25. Inasmuch as the information withheld under Exemption (b)(6) is personal to an individual, there is clearly a privacy interest involved. Therefore, I am required to determine whether there exists any public interest in disclosure, and, if a public interest is implicated, to weigh any such interest against the extent of the invasion to the personal privacy of the individuals.

26. Where Exemption (b)(6) has been applied, I have concluded that: (1) the individuals whose names and/or other personally identifying information has been redacted have a strong privacy interest in not having their personal information released, and that release of this information would constitute a clearly unwarranted invasion of personal privacy because it could result in harassment and unwanted attention; and (2) disclosure of the information would not serve the “core purpose” of the FOIA, *i.e.*, it would not show “what the government is up to.”

The personally identifying information withheld under Exemption (b)(6) consists of Mr. Sanger's cell phone number, an alternate office telephone number, his personal e-mail address, and details about his personal life, another non-Departmental personal e-mail address, and details about two Department employees' personal lives. Accordingly, the privacy interests involved clearly outweigh any public interest in disclosure of such personal information and must, therefore, prevail. This information is therefore exempt from release under FOIA Exemption (b)(6), 5 U.S.C. § 552(b)(6).

IV. DOCUMENT DESCRIPTIONS

27. **C05404110** is a one-page, undated draft of briefing material for a senior Department official who was scheduled to meet with David Sanger. The document is UNCLASSIFIED. The Department withheld the document in its entirety pursuant to FOIA Exemption (b)(5). The release of this document would reveal the preliminary thoughts and ideas determined to be important for preparing a senior official for an interview with a journalist from a major news media organization. Disclosing this document would chill the open and candid assessment that occurs when agency employees are developing a strategy for official action. The Department conducted a line-by-line review of this document and determined that there is no meaningful, non-exempt material that can be reasonably segregated and released. Therefore, the Department properly withheld the document under FOIA Exemption (b)(5), 5 U.S.C. § 552(b)(5), pursuant to the deliberative process privilege.

28. **C05404370** is a five-page, intra-agency e-mail chain consisting of 19 messages among Department officials dated March 1 to March 10, 2012. This e-mail chain forwards a message from Mr. Sanger and pertains to the scheduling of a meeting between Mr. Sanger and Under Secretary of State for Political Affairs Wendy Sherman. The document is

UNCLASSIFIED. The Department withheld a total of three sentences appearing in two messages that contain details of an employee's personal life, as well as Mr. Sanger's personal e-mail address. The Department determined that this employee and Mr. Sanger have privacy interests in this information that outweigh any public interest in disclosure because the withheld information does not shed light on the governmental operations or activities. The Department conducted a line-by-line review of this document and determined that there is no additional meaningful, non-exempt material that can be reasonably segregated and released. Therefore, the Department properly withheld this information under FOIA Exemption (b)(6), 5 U.S.C. § 552(b)(6).

29. **C05404222** is a five-page e-mail chain consisting of 15 messages between Mr. Sanger and Department officials dated December 2 to December 20, 2011. The messages pertain to proposed meetings between Mr. Sanger and several senior Departmental officials. The document is UNCLASSIFIED. The Department withheld only one phrase in one message that pertains to the details of an employee's personal life. The Department determined that this employee has a privacy interest in the withheld information that outweighs any public interest in disclosure because this information does not shed light on governmental operations or activities. For this reason, the Department properly withheld this information pursuant to Exemption (b)(6), 5 U.S.C. § 552 (b)(6). The Department conducted a line-by-line review of this document and determined that there is no additional meaningful, non-exempt material that can be reasonably segregated and released.

30. **C05404149** is a four-page e-mail chain consisting of 10 messages between Mr. Sanger and Assistant Secretary of State for Public Affairs Michael Hammer dated September 12 to October 30, 2011. This exchange pertains to Mr. Sanger's proposed meetings with senior

Department officials. The document is UNCLASSIFIED. The Department withheld only Mr. Sanger's personal e-mail address, cell phone number, and a number where he could be reached at another location. The Department determined that Mr. Sanger has a privacy interest in his personal e-mail address and telephone numbers where he can be reached directly, which outweighs any public interest in disclosure because this information sheds no light on governmental operations or activities. The Department properly withheld this information pursuant to Exemption (b)(6), 5 U.S.C. §552(b)(6). The Department conducted a line-by-line review of this document and determined that there is no additional meaningful, non-exempt material that can be reasonably segregated and released.

31. **C05404362** is a two-page, intra-agency e-mail chain consisting of seven messages on March 2, 2012 between Department officials regarding a proposed meeting between Mr. Sanger and Under Secretary of State for Political Affairs Wendy Sherman. The document is UNCLASSIFIED. The Department withheld only five sentences in one message under Exemption (b)(5) pursuant to the deliberative process privilege. The release of this information would reveal preliminary ideas for preparing a senior official for a meeting with a journalist from a major news media organization. Disclosing this document would chill the open and candid assessment that occurs when agency employees are developing a strategy for official action. The Department conducted a line-by-line review of this document and determined that there is no additional meaningful, non-exempt material that can be reasonably segregated and released. Therefore, the Department properly withheld the information under FOIA Exemption (b)(5), 5 U.S.C. § 552(b)(5), pursuant to the deliberative process privilege.

32. **C05404369** is a five-page, intra-agency e-mail exchange consisting of 20 messages dated March 1, 2012 to March 10, 2012 forwarding a message from Mr. Sanger

regarding the scheduling of a meeting between Mr. Sanger and Under Secretary of State for Political Affairs Wendy Sherman. The document is UNCLASSIFIED. The Department withheld two sentences in one message and one sentence in a different message that contain details of an employee's personal life, as well as Mr. Sanger's personal e-mail address. The Department determined that this employee and Mr. Sanger have privacy interests in this information that outweigh any public interest in disclosure because this information does not shed light on governmental operations or activities. For this reason, the Department properly withheld this information pursuant to Exemption (b)(6), 5 U.S.C. § 552 (b)(6). The Department conducted a line-by-line review of this document and determined that there is no additional meaningful, non-exempt material that can be reasonably segregated and released. Therefore, the Department properly withheld this information under FOIA Exemption (b)(6), 5 U.S.C. § 552(b)(6).

33. **C05404325** is a two-page e-mail chain consisting of eight messages dated January 18 to January 19, 2012 among Department officials and a non-Departmental individual concerning the scheduling of meetings at the State Department. The document is UNCLASSIFIED. The Department withheld only the non-Departmental individual's personal e-mail address. The Department determined that this individual has a privacy interest in his personal e-mail address that outweighs any public interest in this information because it does not shed light on governmental operations. The Department conducted a line-by-line review of this document and determined that there is no additional meaningful, non-exempt material that can be reasonably segregated and released. Therefore, the Department properly withheld the information under FOIA Exemption (b)(6), 5 U.S.C. § 552(b)(6).

34. **C05404185** is a six-page e-mail chain consisting of 14 messages dated December 2 to December 15, 2011 among Department officials and Mr. Sanger regarding proposed appointments for Mr. Sanger with senior Departmental officials. The document is UNCLASSIFIED. The Department withheld only Mr. Sanger's personal e-mail address. The Department determined that Mr. Sanger has a privacy interest in this information that outweighs any public interest in disclosure because this information does not shed light on governmental activities. The Department conducted a line-by-line review of this document and determined that there is no additional meaningful, non-exempt material that can be reasonably segregated and released. Therefore, the Department properly withheld the information under FOIA Exemption (b)(6), 5 U.S.C. § 552(b)(6).

35. **C05404152** is a two-page e-mail chain consisting of three messages dated November 28, 2011 between Mr. Sanger and Assistant Secretary of State for Public Affairs Michael Hammer concerning the scheduling of appointments for Mr. Sanger with senior Department officials. The document is UNCLASSIFIED. The Department withheld only Mr. Sanger's personal e-mail address. The Department determined that Mr. Sanger has a privacy interest in this information that outweighs any public interest because this information does not shed light on governmental activities. The Department conducted a line-by-line review of this document and determined that there is no additional meaningful, non-exempt material that can be reasonably segregated and released. Therefore, the Department properly withheld the information under FOIA Exemption (b)(6), 5 U.S.C. § 552(b)(6).

36. **C05404373** is a two-page e-mail chain consisting of five messages dated March 12–13, 2012 among Department officials and Mr. Sanger regarding arranging an interview with Under Secretary of State for Political Affairs Wendy Sherman. The document is

UNCLASSIFIED. The Department withheld Mr. Sanger's personal e-mail address and one sentence that pertains to Mr. Sanger's personal life. The Department determined that Mr. Sanger has a privacy interest in this information that outweighs any public interest in disclosure because the information does not shed light on the operations of the government. The Department conducted a line-by-line review of this document and determined that there is no additional meaningful, non-exempt material that can be reasonably segregated and released. Therefore, the Department properly withheld the information under FOIA Exemption (b)(6), 5 U.S.C. § 552(b)(6).

37. **C05404372** is a two-page e-mail chain consisting of three messages dated March 12–13, 2012 among Department officials and Mr. Sanger regarding arranging an interview with Under Secretary of State for Political Affairs Wendy Sherman. The document is UNCLASSIFIED. The Department withheld Mr. Sanger's personal e-mail address and one sentence that pertains to Mr. Sanger's personal life. The Department determined that Mr. Sanger has a privacy interest in this information that outweighs any public interest in disclosure because the information does not shed light on governmental operations. The Department conducted a line-by-line review of this document and determined that there is no additional meaningful, non-exempt material that can be reasonably segregated and released. Therefore, the Department properly withheld the information under FOIA Exemption (b)(6), 5 U.S.C. § 552(b)(6).

38. **C05404139** is a seven-page e-mail chain consisting of 20 messages dated December 2, 2011 to January 5, 2012 among Department officials and Mr. Sanger regarding arranging appointments for Mr. Sanger with Department officials. The document is UNCLASSIFIED. The Department withheld only Mr. Sanger's personal e-mail address. The Department determined that Mr. Sanger has a privacy interest in this information that outweighs

any public interest in disclosure because this information does not shed light on governmental operations. The Department conducted a line-by-line review of this document and determined that there is no additional meaningful, non-exempt material that can be reasonably segregated and released. Therefore, the Department properly withheld the information under FOIA Exemption (b)(6), 5 U.S.C. § 552(b)(6).

39. **C05404092** is a three-page e-mail chain consisting of six messages all dated January 6, 2012 among Department officials and Mr. Sanger regarding arranging appointments for Mr. Sanger with Department officials. The document is UNCLASSIFIED. The Department withheld only Mr. Sanger's personal e-mail address. The Department determined that Mr. Sanger has a privacy interest in his personal e-mail address that outweighs any public interest in this information because it does not shed light on governmental operations. The Department conducted a line-by-line review of this document and determined that there is no additional meaningful, non-exempt material that can be reasonably segregated and released. Therefore, the Department properly withheld the information under FOIA Exemption (b)(6), 5 U.S.C. § 552(b)(6).

40. **C05404181** is a seven-page e-mail chain consisting of 11 messages dated December 2 to December 14, 2011 between Mr. Sanger and Assistant Secretary of State for Public Affairs Michael Hammer concerning the scheduling of appointments for Mr. Sanger with senior Department officials. The document is UNCLASSIFIED. The Department withheld only Mr. Sanger's personal e-mail address. The Department determined that Mr. Sanger has a privacy interest in his personal e-mail address that outweighs any public interest in this information because it does not shed light on governmental operations. The Department conducted a line-by-line review of this document and determined that there is no additional meaningful, non-exempt

material that can be reasonably segregated and released. Therefore, the Department properly withheld the information under FOIA Exemption (b)(6), 5 U.S.C. § 552(b)(6).

41. **C05404197** is a six-page e-mail chain consisting of 12 messages dated December 2 to December 19, 2011 among Mr. Sanger and Department officials concerning the scheduling of appointments for Mr. Sanger with senior Department officials. The document is UNCLASSIFIED. The Department withheld only Mr. Sanger's personal e-mail address. The Department determined that Mr. Sanger has a privacy interest in his personal e-mail address that outweighs any public interest in this information because it does not shed light on governmental operations. The Department conducted a line-by-line review of this document and determined that there is no additional meaningful, non-exempt material that can be reasonably segregated and released. Therefore, the Department properly withheld the information under FOIA Exemption (b)(6), 5 U.S.C. § 552(b)(6).

42. **C05404351** is a two-page e-mail chain consisting of six messages dated March 1 to March 2, 2012 among Mr. Sanger and Department officials concerning the scheduling of appointments for Mr. Sanger with senior Department officials. The document is UNCLASSIFIED. The Department withheld only Mr. Sanger's personal e-mail address. The Department determined that Mr. Sanger has a privacy interest in his personal e-mail address that outweighs any public interest in this information because it does not shed light on governmental operations. The Department conducted a line-by-line review of this document and determined that there is no additional meaningful, non-exempt material that can be reasonably segregated and released. Therefore, the Department properly withheld the information under FOIA Exemption (b)(6), 5 U.S.C. § 552(b)(6).

43. **C05404358** is a three-page e-mail chain consisting of 12 messages dated March 1 to March 2, 2012 among Mr. Sanger and Department officials concerning the scheduling of appointments for Mr. Sanger with senior Department officials. The document is UNCLASSIFIED. The Department withheld only Mr. Sanger's personal e-mail address. The Department determined that Mr. Sanger has a privacy interest in his personal e-mail address that outweighs any public interest in this information because it does not shed light on governmental operations. The Department conducted a line-by-line review of this document and determined that there is no additional meaningful, non-exempt material that can be reasonably segregated and released. Therefore, the Department properly withheld the information under FOIA Exemption (b)(6), 5 U.S.C. § 552(b)(6).

44. **C05404364** is a four-page e-mail chain consisting of 15 messages dated March 1 to March 2, 2012 among Mr. Sanger and Department officials concerning the scheduling of appointments for Mr. Sanger with senior Department officials. The document is UNCLASSIFIED. The Department withheld only Mr. Sanger's personal e-mail address. The Department determined that Mr. Sanger has a privacy interest in his personal e-mail address that outweighs any public interest in this information because it does not shed light on governmental operations. The Department conducted a line-by-line review of this document and determined that there is no additional meaningful, non-exempt material that can be reasonably segregated and released. Therefore, the Department properly withheld the information under FOIA Exemption (b)(6), 5 U.S.C. § 552(b)(6).

45. **C05404366** is a four-page e-mail chain consisting of 16 messages dated March 1 to March 7, 2012 among Mr. Sanger and Department officials concerning the scheduling of appointments for Mr. Sanger with senior Department officials. The document is

UNCLASSIFIED. The Department withheld only Mr. Sanger's personal e-mail address. The Department determined that Mr. Sanger has a privacy interest in his personal e-mail address that outweighs any public interest in this information because it does not shed light on governmental operations. The Department conducted a line-by-line review of this document and determined that there is no additional meaningful, non-exempt material that can be reasonably segregated and released. Therefore, the Department properly withheld the information under FOIA Exemption (b)(6), 5 U.S.C. § 552(b)(6).

46. **C05389507** is a three-page, intra-agency e-mail chain consisting of 10 messages dated December 15, 2011 to January 5, 2012 among Department officials trying to arrange a meeting between Mr. Sanger and Deputy Secretary of State William Burns. The document is UNCLASSIFIED. The Department withheld only two sentences and one phrase in one message under Exemption (b)(5) pursuant to the deliberative process privilege. The release of this information would reveal preliminary ideas for preparing a senior official for a meeting with a journalist from a major news media organization. Disclosing this document would chill the open and candid assessment that occurs when agency employees are developing a strategy for official action. The Department conducted a line-by-line review of this document and determined that there is no additional meaningful, non-exempt material that can be reasonably segregated and released. Therefore, the Department properly withheld the information under FOIA Exemption (b)(5), 5 U.S.C. § 552(b)(5), pursuant to the deliberative process privilege.

47. **C05406079** is a one-page, intra-agency e-mail chain consisting of three messages dated March 2, 2012 among Department officials concerning a proposed meeting between Mr. Sanger and Under Secretary of State for Political Affairs Wendy Sherman. The document is UNCLASSIFIED. The Department withheld only five sentences in one message under

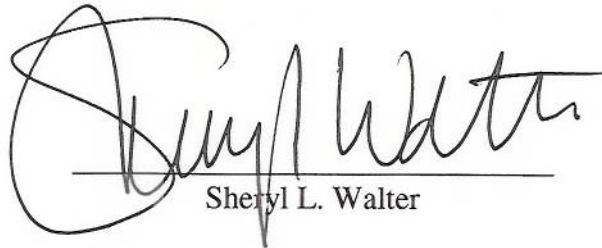
Exemption (b)(5) pursuant to the deliberative process privilege. The release of this information would reveal preliminary ideas for preparing a senior official for a meeting with a journalist from a major news media organization. Disclosing this document would chill the open and candid assessment that occurs when agency employees are developing a strategy for official action. The Department conducted a line-by-line review of this document and determined that there is no additional meaningful, non-exempt material that can be reasonably segregated and released. Therefore, the Department properly withheld the information under FOIA Exemption (b)(5), 5 U.S.C. § 552(b)(5), pursuant to the deliberative process privilege.

CONCLUSION

48. In summary, the Department conducted a thorough search of all components that it determined had a reasonable possibility of possessing records responsive to item 2 of Plaintiff's FOIA request related to the June 1, 2013 New York Times article. As a result of the supplemental searches described in this declaration, the Department located 76 additional responsive records. The Department released 55 of these records in full and 20 records in part to Plaintiff and withheld one record in full.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Executed this 30th day of July 2013, Washington, D.C.



Sheryl L. Walter

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

FREEDOM WATCH, INC.,

Plaintiff,

v.

Case No. 1:12-cv-01088 (CRC)

NATIONAL SECURITY AGENCY,
CENTRAL INTELLIGENCE AGENCY,
DEPARTMENT OF DEFENSE, and
DEPARTMENT OF STATE,

Defendants.

ORDER

For the reasons stated in the Court's accompanying memorandum opinion, it is hereby

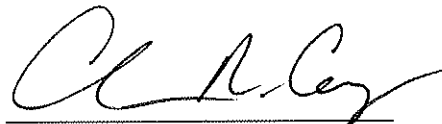
ORDERED that Defendant's motion for summary judgment [Dkt. No. 11] is granted.

This is a final, appealable order.

SO ORDERED.

Date:

6/12/14



CHRISTOPHER R. COOPER
United States District Judge

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

FREEDOM WATCH, INC.,

Plaintiff,

v.

NATIONAL SECURITY AGENCY,
CENTRAL INTELLIGENCE AGENCY,
DEPARTMENT OF DEFENSE, and
DEPARTMENT OF STATE,

Defendants.

Case No. 1:12-cv-01088 (CRC)

MEMORANDUM OPINION

Freedom Watch, Inc., challenged the responses of four federal agencies to its Freedom of Information Act (“FOIA”) requests regarding a 2012 *New York Times* article discussing a U.S. cyber-attack on Iran. After the Court ruled in favor of three of the agencies on the pleadings, and dismissed claims against the State Department with respect to all but one category of requested records, the State Department conducted a rolling search for records responsive to Freedom Watch’s lone remaining request. Because the Department’s affidavits establish that it conducted an adequate search, and Freedom Watch has not provided any evidence to the contrary, the Court will grant the Department’s motion for summary judgment.

I. Background

The genesis of this dispute is a June 1, 2012 *New York Times* article by David Sanger describing the Bush and Obama Administrations’ classified program to undermine Iran’s nuclear program by releasing a computer “worm” within that country’s main nuclear enrichment plant. Compl. Ex. 1. Sanger reportedly based his account of the initiative—dubbed “Olympic Games”—on interviews with “current and former American, European and Israeli officials involved in the program, as well as a range of outside experts.” *Id.* Freedom Watch believed that classified

information about the program had been leaked by “Obama Administration sources on the President’s behalf . . . to further [his] 2012 re-election campaign[,]” notwithstanding the multiple other potential sources for the information contained in the article. Id. Expressing alarm that these suspected leaks had jeopardized national security and hastened a confrontation between Iran and Israel, Freedom Watch submitted requests under the Freedom of Information Act, 5 U.S.C. § 552, to the Department of Defense (“DOD”), the Central Intelligence Agency (“CIA”), the National Security Agency (“NSA”), and the State Department. The requests sought: (1) information relating to the article, including classified information that was allegedly leaked to Sanger; (2) records relating to information released to Sanger; (3) information on whomever provided information to Sanger; (4) communications with the White House regarding the article; (5) information related to “the decision to ‘leak’”; and (6) information on any government investigations into the article. Id. ¶ 4.

After waiting the required 20 days, see 5 U.S.C. § 552(a)(6)(A), Freedom Watch filed suit to compel the four agencies to search for and produce responsive records. The NSA and the CIA moved for judgment on the pleadings and the DOD moved for summary judgment, each of which the Court granted, resolving all claims in favor of those agencies. Order (Dec. 13, 2012). The Court also granted the State Department’s motion for judgment on the pleadings with respect to requests 1 and 3–6, finding the requests to be overly speculative, but denied it as to Freedom Watch’s second request, regarding information released to Sanger. Id.

After the partial dismissal, and while summary judgment briefing was still ongoing, the State Department conducted several searches for records responsive to Freedom Watch’s second request. The Department’s searches are detailed in declarations provided by Sheryl L. Walter, Director of the Department’s Office of Information Programs and Services (“IPS”). According to Ms. Walter, IPS evaluated Freedom Watch’s request “to determine which offices, overseas posts, or

records systems within the Department may be reasonably expected to contain the records requested.” Supplemental Walter Decl. ¶ 1. This selection process was based on “the holdings of the Department’s records systems, applicable records disposition schedules, and the substantive and functional mandates of numerous Department offices and Foreign Service posts and missions” as well as the “nature, scope, and complexity of the request.” Id. ¶ 10. IPS identified three “offices or records systems with a reasonable possibility of possessing responsive documents”: the Central Foreign Policy Records, which, as the name suggests, is the central record system at the Department; the Bureau of Public Affairs, which is charged with managing communications between the Department and the media; and the Bureau of Near Eastern Affairs, which “advis[es] the Secretary of State on matters in North Africa and the Middle East.” Id. ¶¶ 12–18.

With relevant locations for the search determined, Department employees began by conducting full text searches of the electronic record systems in each department—including individual electronic records of all employees in the Bureau of Public Affairs and 15 employees in the Bureau of Near Eastern Affairs’ Iran office—for the terms “David Sanger” and “David E. Sanger.” Id. ¶¶ 14, 17, 19. The Near Eastern Affairs Bureau’s Iran office also searched physical records that its employees knew to be excluded from the electronic records system and had a “reasonable possibility of containing information responsive to this FOIA request.” Id. ¶ 19. These initial searches identified no responsive documents except in the Bureau of Public Affairs, which discovered three records, two of which the Department released in full and one it released in part after redacting material it deemed nonresponsive. Id. ¶¶ 9, 14, 17, 19.

After receiving Freedom Watch’s opposition to its summary judgment motion, the Department voluntarily asked the Bureau of Public Affairs to confirm that no other locations should be searched. In response, the Bureau determined that it had neglected to search its front office, which performs executive tasks to support the Bureau. Second Supplemental Walter Decl. ¶ 6.

Due to its discovery of additional potentially responsive records, the Department sought and was granted a 60-day extension of time to conduct a supplemental search and reply to Freedom Watch's opposition brief. Order (June 5, 2013). Employees of the Bureau conducted a search of the front office's paper records and searched its electronic records for the term "Sanger," uncovering 62 responsive documents. These documents revealed that Sanger had interviewed five State Department employees. *Id.* ¶¶ 7–9. The Department then searched the records of those five employees and their respective departments—by manual search of paper records and full-text search of electronic records for the term "Sanger"—discovering 14 additional documents. *Id.* ¶¶ 10–19. Since the beginning of this suit, the State Department has produced a total of 79 documents responsive to Freedom Watch's FOIA request, releasing 58 in full, 20 in part, and withholding one in full. *Id.* ¶¶ 3, 48.

In the midst of the Department's voluntary supplemental search, Freedom Watch moved to depose a State Department records custodian concerning the adequacy of the original search, which Freedom Watch suggested was part of a pattern of "outright obstruction of justice" by the Obama Administration. Mot. for Discovery at 1. Judge Wilkins denied the motion, finding no evidence of bad faith on the part of Department, but invited Freedom Watch to renew its request after the Department had an opportunity to fully explain the adequacy of its search. Minute Order (June 18, 2013). Freedom Watch has declined to renew its motion or to challenge the Department's supplemental production.

II. Standard of Review

The Court may grant summary judgment if "the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). The Court must accept the non-movant's evidence as true and draw all reasonable inferences in favor of the non-moving party. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 255

(1986). “FOIA cases typically and appropriately are decided on motions for summary judgment.” Defenders of Wildlife v. U.S. Border Patrol, 623 F. Supp. 2d 83, 87 (D.D.C. 2009); accord Brayton v. Office of the U.S. Trade Representative, 641 F.3d 521, 527 (D.C. Cir. 2011). Summary judgment in the FOIA context requires the government to “demonstrate the absence of a genuine dispute regarding the adequacy of its search for or production of responsive records.” Judicial Watch, Inc. v. Dep’t of the Navy, 971 F. Supp. 2d 1, 3 (D.D.C. 2013) (citing Nat’l Whistleblower Ctr. v. Dep’t of Health & Human Servs., 849 F. Supp. 2d 13, 21–22 (D.D.C. 2012)).

III. Analysis

A. Adequacy of the State Department’s Search

To meet its FOIA obligations, an agency must show that it “conducted a search reasonably calculated to uncover all relevant documents.” Weisberg v. Dep’t of Justice, 705 F.2d 1344, 1351 (D.C. Cir. 1983). The agency is not required to prove that it discovered every possibly relevant document, id. at 1485, but simply must demonstrate “a good faith effort[.]” Oglesby v. Dep’t of the Army, 920 F.2d 57, 68 (D.C. Cir. 1990). The Court will judge the adequacy of an agency’s search for documents by a standard of reasonableness that “depends, not surprisingly, upon the facts of each case.” Weisberg, 705 F.2d at 1485.

The Court may grant summary judgment on the basis of agency affidavits and declarations alone when they are “relatively detailed and non-conclusory.” SafeCard Servs., Inc. v. SEC, 926 F.2d 1197, 1200 (D.C. Cir. 1991). The affidavits need not “set forth with meticulous documentation the details of an epic search for the requested records[.]” Perry v. Block, 684 F.2d 121, 127 (D.C. Cir. 1982). But they must describe “what records were searched, by whom, and through what processes,” Steinberg v. Dep’t of Justice, 23 F.3d 548, 551–52 (D.C. Cir. 2008) (citing Weisberg v. Dep’t of Justice, 637 F.2d 365, 371 (D.C. Cir. 1980)), and should “set[] forth the search terms and the type of search performed and aver[] that all files likely to contain

responsive materials . . . were searched.” Ogelsby, 920 F.2d at 68. There is a presumption of good faith accorded to agency submitted affidavits or declarations, “which cannot be rebutted by ‘purely speculative claims about the existence and discoverability of other documents.’” SafeCard Servs., 926 F.2d at 1200 (quoting Ground Saucer Watch, Inc. v. CIA, 692 F.2d 770, 771 (D.C. Cir. 1981)).

The State Department has demonstrated that it conducted an adequate search for records responsive to Freedom Watch’s FOIA request. Ms. Walter’s declarations indicate the places that were searched and explain why the Department determined that those records systems were likely to contain responsive documents. IPS searched the central record system for the State Department as a whole, the record systems of the bureau that manages communications with the media, and the bureau that oversees policy in Iran, the country to which Sanger’s article relates. Supplemental Walter Decl. ¶¶ 12–13, 14, 18. These are perfectly logical locations to search for potentially responsive records. Walter’s declarations further explain that the terms “David Sanger” and “Sanger” were used to search relevant electronic records and that physical files were reviewed by knowledgeable staff. Id. ¶¶ 14, 17, 19; Second Supplemental Walter Decl. ¶¶ 7–9. Searching by Sanger’s name was a reasonable method of uncovering documents regarding what information employees may have given him; indeed, Freedom Watch does not quarrel with the search methods used. Additionally, when IPS realized it had neglected to search other relevant record systems or when documents suggested that other individuals might have responsive records, the Department responded by conducting further searches and providing Freedom Watch additional responsive records. Second Supplemental Walter Decl. ¶¶ 7–19. Notably, Freedom Watch does not object to the adequacy of the supplemental searches conducted after it filed its opposition.

Freedom Watch may overcome the presumption of good faith accorded the State Department’s declarations by presenting countervailing evidence, see Iturralde v. Comptroller of the Currency, 315 F.3d 311, 314 (D.C. Cir. 2003), but it has not done so. It offers instead

speculative, unsupported assertions that do not call into question the adequacy of the State Department's search. It posits, for example, that Sanger must have received the information for the article directly from former Secretary of State Hillary Clinton, and that "someone was undoubtedly present at the interview and was responsible for taking notes, preparing memoranda, and/or preparing some sort of record of the Secretary of State's statements." Pl.'s Opp. to Mot. for Summ. J. at 2, 6–8. These allegations, lacking any evidentiary support, are insufficient to contradict the comprehensive description of the search set forth in the Walter declarations. See SafeCard Servs., 926 F.2d at 1201 ("Mere speculation that as yet uncovered documents may exist does not undermine the finding that the agency conducted a reasonable search for them." (citation omitted)). Moreover, the Court determines adequacy "not by the fruits of the search, but by the appropriateness of the methods used to carry out the search." Iturralde, 315 F.3d at 315.

Freedom Watch also questions the adequacy of the State Department's search because the lion's share of responsive documents was found only as a result of corrective searches. Pl.'s Opp. to Mot. For Summ. J. at 3–4. But "it does not matter that an agency's *initial* search failed to uncover certain responsive documents so long as subsequent searches captured them." Hodge v. FBI, 703 F.3d 575, 580 (D.C. Cir. 2013) (emphasis in original). Unless Freedom Watch "can identify any additional searches that must be conducted," id., which it has declined to do, the State Department has met its burden by conducting searches that were reasonably calculated to find responsive records, regardless of whether the records were found initially or after subsequent searches.

Finally, Freedom Watch argues that because IPS referred one document to another agency for review and redaction, Walters lacks "the requisite personal knowledge as to" whether the document was responsive or was appropriately redacted. Pl.'s Opp. to Mot. for Summ. J. at 6–7. Walter's supplemental declaration explains that the document in question originated with the

National Security Staff (“NSS”), now called the National Security Council, which requested the redaction of nonresponsive sections. Second Supplemental Walter Decl. ¶¶ 3–4. Walter, as IPS’s director, had sufficient personal knowledge of the document’s content because IPS initially discovered the document before sending it to NSS, which then requested redactions that *IPS* performed. *Id.* She also adequately justifies withholding parts of the document, explaining that the redacted information discussed issues that were of media interest at the time but were not related to the subject of Freedom Watch’s request. *Id.* The practice of redacting non-responsive materials from documents produced in response to FOIA requests has been approved by courts in this Circuit. See, e.g., Meniffee v. Dep’t of the Interior, 931 F. Supp. 2d 149, 167 (D.D.C. 2013); Pinson v. Lappin, 806 F. Supp. 2d 230, 237 (D.D.C. 2011); Wilson v. Dep’t of Transp., 730 F. Supp. 2d 140, 156 (D.D.C. 2010), aff’d, 10-5295, 2010 WL 5479580 (D.C. Cir. Dec. 30, 2010).¹

In summary, the State Department has submitted “reasonably detailed” declarations “setting forth the search terms and the type of search performed, and averring that all files likely to contain responsive materials (if such records exist) were searched[.]” Oglesby, 920 F.2d at 68. Because Freedom Watch has not offered evidence to counter the Department’s declarations, the State Department has satisfied its burden to establish that it conducted an adequate search in response to Freedom Watch’s FOIA request.

¹ Freedom Watch also argues that it cannot know if the search was adequate without knowing how many subsidiary departments actually exist within the State Department and expresses skepticism that “a large federal agency throughout the world[] only has two databases from which to search.” Pl.’s Opp. to Mot. for Summ. J. at 7. As stated above, however, mere speculation that other record systems should exist does not contradict the State Department’s affidavits explaining why certain record systems were determined likely to contain responsive records. See SafeCard Servs., 926 F.2d at 1201. The Court also notes that the State Department’s website provides a publically available chart of its subsidiary departments. Department Organization Chart: March 2014, U.S. Department of State, <http://www.state.gov/r/pa/ei/rls/dos/99494.htm> (last visited June 12, 2014).

B. The State Department's Vaughn Index

In addition to challenging the adequacy of the State Department's search, Freedom Watch argues in its opposition that the Department failed to create a Vaughn index for the withheld documents. Pl.'s Opp. to Mot. for Summ. J. at 8–9. The only document withheld when Freedom Watch filed its opposition was the NSS document, which, as explained above, the State Department adequately justified redacting. After conducting supplemental searches, the State Department withheld several other documents in whole or in part, but detailed for each record the type of document, the author of the document, a general description of the contents of the document, and the basis for the exemption being claimed. See Second Supplemental Walter Decl. ¶¶ 20–47. “[A]n agency does not have to provide an index per se, but can satisfy its burden by other means, such as . . . providing a detailed affidavit or declaration.” Voinche v. FBI, 412 F. Supp. 2d 60, 65 (D.D.C. 2006) (citing Gallant v. NLRB, 26 F.3d 168, 172 (D.C. Cir. 1994)). The descriptions in Walter's declaration “give the reviewing court a reasonable basis to evaluate the claim of privilege,” Gallant, 26 F.3d at 172–73, and thus adequately support the State Department's withholdings.

C. Exemption 5

FOIA Exemption 5 shields from disclosure “inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency.” 5 U.S.C. § 522(b)(5). Exemption 5 encompasses the deliberative process privilege, which protects “documents reflecting advisory opinions, recommendations and deliberations comprising part of a process by which governmental decisions and policies are formulated.” Dep't of Interior v. Klamath Water Users Protective Ass'n, 532 U.S. 1, 8 (2001) (quoting NLRB v. Sears, Roebuck & Co., 421 U.S. 132,150 (1975)). The purpose behind the privilege—and thus Exemption 5—is “to enhance the quality of agency decisions by protecting open and frank discussion among those who

make them within the Government.” Id. at 9.

Pursuant to Exemption 5, the State Department withheld portions of three documents and all of one document because they contained briefing material for senior department officials with “preliminary thoughts and ideas determined to be important for preparing [the] senior official[s] for an interview with a journalist from a major news media organization.” Second Supplemental Walter Decl. ¶¶ 27, 31, 46, 47. Because these documents reflect intra-agency deliberations on communications with the media, they fall within the deliberative process privilege and are covered under Exemption 5. See Judicial Watch, Inc. v. Dep’t of Commerce, 337 F. Supp. 2d 146, 174 (D.D.C. 2004) (agency properly withheld “talking points and recommendations for how to answer questions . . . prepared by [agency] employees for the consideration of [agency] decision-makers”); see also Competitive Enter. Inst. v. EPA, 12-1617, 2014 WL 308093, at *10–11 (D.D.C. Jan. 29, 2014) (Exemption 5 held to protect “media-related withholdings . . . reflect[ing] ongoing decisionmaking about ‘how the agency’s activities should be described to the general public’”).

D. Exemption 6

FOIA Exemption 6 allows agencies to withhold “personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.” 5 U.S.C. § 552(b)(6). “Similar files” broadly include documents containing “purely personal information.” See, e.g., Gov’t Accountability Project v. Dep’t of State, 699 F. Supp. 2d 97, 106 (D.D.C. 2010) (citing Dep’t of State v. Wash. Post Co., 456 U.S. 595, 602 (1982)).

The State Department withheld information in 17 documents provided to Freedom Watch pursuant to Exemption 6 because the redacted information consisted of personal email addresses, phone numbers, and details of individuals’ personal lives. Second Supplemental Walter Decl. ¶¶ 28–30, 32–45. Such “purely personal information” clearly falls within Exemption 6.

IV. Conclusion

For the foregoing reasons, the Court will grant the State Department's motion for Summary Judgment. The Court will issue an order in accordance with this Memorandum Opinion.

Date: June 12, 2014



CHRISTOPHER R. COOPER
United States District Judge

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

FREEDOM WATCH, INC.

Plaintiff,

v.

**NATIONAL SECURITY AGENCY, ET.
AL.,**

Defendants.

Civil Action No. 1:12-cv-01088-CRC

NOTICE OF APPEAL

NOTICE is hereby given that Plaintiff Freedom Watch appeals to the United States Court of Appeals for the District of Columbia Circuit from the Order and Memorandum Opinion of this Court entered on June 12, 2014 (Docket Nos. 24,25)(Exhibit 1,2), which granted summary judgment to the Defendants, and all other orders and rulings adverse to Plaintiff in this case.

Dated: July 14, 2014

Respectfully Submitted,

/s/ Larry Klayman

Larry Klayman, Esq.
FREEDOM WATCH, INC.
D.C. Bar No. 334581
2020 Pennsylvania Ave. NW #345
Washington, DC 20006
Tel: (310) 595-0800
Email: leklayman@gmail.com

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 14th day of July, 2014 a true and correct copy of the foregoing Notice of Appeal (Case No. 1:12-cv-1088) was submitted electronically to the U.S. District Court for the District of Columbia and served via CM/ECF upon the following:

John K. Theis
Trial Attorney
Federal Programs Branch
U.S. Department of Justice, Civil Division
20 Massachusetts Avenue, NW
Room 6107
Washington, DC 20530
John.K.Theis@usdoj.gov

Attorney for Defendants.

Respectfully Submitted,

/s/ Larry Klayman
Larry Klayman, Esq.
FREEDOM WATCH, INC.
D.C. Bar No. 334581
2020 Pennsylvania Ave. NW #345
Washington, DC 20006
Tel: (310) 595-0800
Email: leklayman@gmail.com

CERTIFICATE OF SERVICE

I hereby certify that on December 31, 2104, I caused the foregoing document to be electronically filed with the Clerk of the Court for the United States Court of Appeals for the D.C. Circuit by using the appellate CM/ECF system. I further certify that on the same day, I served the foregoing document on the following counsel by electronic service via the CM/ECF system:

Catherine H. Dorsey, Attorney
Email: catherine.dorsey@usdoj.gov
U.S. Department of Justice
(DOJ) Office of the Attorney General
950 Pennsylvania Avenue, NW
Washington, DC 20530

Matthew M. Collette, Attorney
Email: Matthew.Collette@usdoj.gov
U.S. Department of Justice
(DOJ) Civil Division, Appellate Staff
Firm: 202-514-2000
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

Attorneys for Defendants-Appellees.

Respectfully Submitted,

/s/ Larry Klayman

Larry Klayman, Esq.
D.C. Bar No. 334581
Freedom Watch, Inc.
2020 Pennsylvania Ave. NW, Suite 345
Washington, DC 20006
Tel: (310) 595-0800
Email: leklayman@gmail.com