

FILED 26 JUL '12 13:13 USDC-ORE

UNITED STATES DISTRICT COURT

THE DISTRICT OF OREGON

EUGENE DIVISION

Diane Roark,
Plaintiff

:

Case No.: 6:12-1354-AA

v.

:

Violations of Constitutional Rights
Return of Property, Rule 41(g)

United States,
Defendant.

:

...oOo...

COMPLAINT

Parties

1. Plaintiff Diane Roark, filing *pro se*, resides in Stayton, Oregon and is a citizen of the United States.

2. The Defendant is the United States, due to actions and omissions by the National Security Agency (NSA), headquartered at Ft. George G. Meade, Maryland, and the Federal Bureau of Investigation (FBI) and Department of Justice (DOJ), each headquartered in Washington, D.C.

Jurisdiction

3. Plaintiff's property was seized by the FBI from her residence in Stayton, Oregon, in Marion County, which falls under jurisdiction of the Eugene Division. Plaintiff was removed for improper venue from a Rule 41(g) lawsuit filed by five parties in the United States District Court of Maryland, and was notified that the proper venue in her case is the United States District Court of Oregon. *Wiebe et al. v National Security Agency et al.*,

600007619

Civil Case No. RDB-11-3245.

Facts

4. Plaintiff was employed at the House Permanent Select Committee on Intelligence, and was responsible for oversight of NSA's operations and budget for the five years before her retirement in April, 2002. Plaintiff was suspected of providing classified government information about "warrantless wiretaps" to the New York Times (NYT), and to NYT reporter James Risen for a book on the same topic, published in December 2005 and January 2006 respectively, and/or to the Baltimore Sun. Plaintiff voluntarily met with the U.S. Attorney and FBI investigators for three hours in February, 2007. She answered all their questions, except she refused to reveal her sources of information on warrantless wiretaps, and details of her discussion with a congressman, citing congressional privilege under the constitutional Separation of Powers. She also provided an Affidavit swearing that she was not the source of the NYT or Risen exposes on "warrantless wiretaps." Three persons have publicly admitted to being sources for information on warrantless wiretaps published in the NYT and elsewhere, but none of them have been prosecuted.

5. The FBI raided Roark's property on July 26, 2007, seizing many boxes of papers, rolodexes and electronic equipment. Simultaneous raids took place in Maryland at the homes of two associates, J.K. Wiebe and William Binney. At the same time, another associate, Edward Loomis, was removed from his place of employment and "persuaded" to allow a search of his home without a warrant. A fourth associate, Thomas Drake, was raided on November 28, 2007. Loomis and Drake lost high-paying jobs. All of us lost our security clearances and opportunity for further employment in our field of expertise.

6. In December, 2009, prosecutors deliberately lied, claiming that Plaintiff committed felony perjury in her interview nearly three years earlier, and offered her a plea bargain; Plaintiff refused the plea bargain and exposed the lie. She has heard nothing about her case since then, despite a number of requests in 2012 for written notification of her status. Two associates were officially notified in January/February, of 2010 that they were no longer targets and were offered letters of immunity; a third associate was provided the same assurances in October, 2010. Thomas Drake was indicted in April, 2010, but all ten felony charges were dropped four days before his trial, scheduled for June, 2011. Prosecutors agreed that no classified information was revealed in the Baltimore Sun articles. *United States v. Drake*, 2011 WL 2175007 at *5 (D. Md. 2011).

7. The five associates' seized property was not returned despite ten requests over four years by Loomis and two requests submitted by Wiebe and Binney after the Drake case was settled (Drake's public defenders managed to get a small amount of his property returned). Therefore, all five associates filed a joint Maryland civil lawsuit in November, 2011. Some property was returned to the associates, including Plaintiff, under pretrial negotiations supervised by a Magistrate Judge, but computers and their contents and some electronic storage devices were not returned; many of Plaintiff's papers also were retained. Defendants maintained that review of each remaining computer hard drive and storage device for classified data or for unclassified data that had not been released officially by NSA would last at least six months and in the case of one hard drive, 13 man-months, perhaps consecutively. Incongruously, the Government simultaneously asserted that all retained property did contain government information that was protected by the National Security Agency Act of 1959 (NSAA), some of which was classified.

Plaintiffs accepted the option offered by the Magistrate Judge to proceed with the trial.

8. The Maryland Defendants moved for dismissal or, in the alternative, summary judgment, and noted that Plaintiff's venue was improper. Plaintiff was removed from the case in May, 2012. A hearing on the Defendants' motion is scheduled for August 23, 2012. The five-year statute of limitations for Plaintiff to file a return-of-property lawsuit in Oregon under Rule 41(g) is July 26, 2012.

9. In a motion and response related to the Government's Motion to Dismiss, the Government argues, *inter alia*, that:

- as a matter of "*NSA policy*" and under Article 6 of the NSAA, if a hard drive or storage device contains even one document with classified information, or with unclassified information about NSA that has not been officially released, the entire hard drive or storage device will not be returned to its owner.
- this "government information" is "government property" that the government has an "unquestioned right" to protect; further, such property is contraband; further, Rule 41(g) requires that the petitioner be entitled to lawful possession of the seized property and that seized property cannot be contraband; and further, because the Petitioners had no right to possess government property, they do not come to court with "clean hands." As a result, Petitioners lack standing. In addition, the Government contended that in a civil case, the judge has no authority to review NSA's classification decisions.
- To Plaintiffs' arguments that some asserted NSA rights are unconstitutional, Defendants responded that a Rule 41(g) case is not a constitutional case.

10. Plaintiffs argued in the Maryland case, *inter alia*, that

- growing evidence indicated that prior to raiding Plaintiff and her associates,

agents of the Government had conducted a surreptitious search of Roark's property, thereby acquiring information about her associations and activities. Data from that search apparently was used to secure warrants for the subsequent search and seizures at Plaintiff's property and the properties of Wiebe, Binney and Drake, and to justify the warrantless search and seizure of Loomis' property. Affidavits for the warrants remain sealed. Plaintiff has never been notified of a surreptitious search of her property, as required by law and in violation of the Fourth Amendment. Searches based on information from an illegal search, the Maryland Plaintiffs argued, were unconstitutional use of the "fruit of the poisonous tree." Further, property seized during a search pursuant to a prior illegal search must be returned.

- Government assertion of sweeping rights to withhold any unclassified information that is not officially released by NSA and even to refuse to return voluminous other undisputed information located on an electronic device with such unclassified (or classified) information, violates citizen rights to free speech and communication under the First Amendment and to private property under the Fourth Amendment [as well as the Fifth and Sixth Amendments].

Requests for Relief

11. Plaintiff asks that the Court find unconstitutional the following Government actions and claims:

- the Government's activities and assertions described in paragraphs 9 and 10 that infringe on citizen speech and communications under the First Amendment to the Constitution and on property rights under the Fourth, Fifth and Sixth Amendments.
- the manner in which the Government investigated, managed and prolonged her

case. Plaintiff contends that the actions taken against her constitute retaliation for her whistleblower activities and execution of her Congressional oversight responsibilities that revealed inefficiency, contract fraud, the persistent waste of billions of dollars on a single ill-conceived program that was never built, plus illegal and unconstitutional operations. Plaintiff requests that the Court declare that the Government violated her Fourth Amendment rights through illegal search and seizure and possibly other secret means; her Fifth Amendment rights to due process, through lengthy persecution, attempted malicious prosecution, abuse of process and intentional infliction of emotional distress; and her Sixth Amendment right to a speedy trial or notification of immunity, plus to be informed of the nature and cause of the accusation and confronted with the witnesses and evidence against her.

Plaintiff seeks to prevent government agencies from repeating these assaults against other citizens based on whim and retribution even after the Government lacks facts to support a prosecution, and to provide a legal precedent and recourse for victims of any such unconscionable acts. Further, since the government sought in this case to quash the exposure of waste, fraud, abuse and illegality in national security programs, the inherent secretiveness of which helps hide problems from citizen review, Plaintiff prays that the Court will uphold the right of employees and citizens to responsible whistleblowing when other alternatives are unavailable or ineffective.

12. Plaintiff requests that the Court direct the Government to refrain from withholding from the public for prolonged and indefinite periods information that is not classified, and that it direct the Information Security Oversight Office to conform, circumscribe and sunset the various agency uses of designations for unclassified information, such as

FOUO (For Official Use Only), within twelve months of its ruling. Legitimately unclassified information should not be withheld from the public, particularly if it is being withheld because it would expose Agency errors and wrongdoing.

13. If FISA requirements for physical searches and/or electronic surveillance are found to have been intentionally violated under the color of law, Plaintiff requests invocation of the statute's cause of action clause imposing criminal and civil liabilities, penalties, damages and punitive damages, and awarding attorney's fees.

14. Finally, Plaintiff seeks return of her remaining property, except those items that she has said need not be returned, if necessary under an associated Rule 41(g) action following resolution of constitutional issues.

15. WHEREFORE, the Plaintiff demands judgment against the Defendant and such other relief as this Court deems just.

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

Signed this 25th day of July, 2012.

Signature	
Name	Diane Roark
Address	2000 N. Scenic View Dr. Stayton, OR 97383
Telephone	503-767-2490

Certificate of Service

I HEREBY CERTIFY that on July 26, 2012, a copy of a Complaint against the United States Government for violation of the First, Fourth, Fifth and Sixth Amendments to the Constitution and for Return of Property (including a Rule 41(g) action if necessary), was sent, postage prepaid and certified mail to:

Mr. Eric Holder
Attorney General of the United States
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530-0001

Another copy was hand delivered to:

U.S. Attorney's Office, District of Oregon
405 E. 8th Ave., Suite 2400
Eugene, Oregon 97401

 *Diane Roark, pro se*

Diane Roark
2000 N. Scenic View Dr.
Stayton, Oregon 97383
503-767-2490

JS 44 (Rev. 09/11)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS

(b) County of Residence of First Listed Plaintiff Marion
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number)
pro se

DEFENDANTS

REC'D 26 JUL '12 13:13 USDC-ORE

County of Residence of First Listed Defendant _____
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- 1 U.S. Government Plaintiff
- 3 Federal Question (U.S. Government Not a Party)
- 2 U.S. Government Defendant
- 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

- | | | | | | |
|---|----------------------------|----------------------------|---|----------------------------|----------------------------|
| Citizen of This State | <input type="checkbox"/> 1 | <input type="checkbox"/> 1 | Incorporated or Principal Place of Business In This State | <input type="checkbox"/> 4 | <input type="checkbox"/> 4 |
| Citizen of Another State | <input type="checkbox"/> 2 | <input type="checkbox"/> 2 | Incorporated and Principal Place of Business In Another State | <input type="checkbox"/> 5 | <input type="checkbox"/> 5 |
| Citizen or Subject of a Foreign Country | <input type="checkbox"/> 3 | <input type="checkbox"/> 3 | Foreign Nation | <input type="checkbox"/> 6 | <input type="checkbox"/> 6 |

IV. NATURE OF SUIT (Place an "X" in One Box Only)

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES	
<input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 151 Medicare Act <input type="checkbox"/> 152 Recovery of Defaulted Student Loans (Excl. Veterans) <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input type="checkbox"/> 160 Stockholders' Suits <input type="checkbox"/> 190 Other Contract <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise	PERSONAL INJURY <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Federal Employers' Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input type="checkbox"/> 360 Other Personal Injury <input type="checkbox"/> 362 Personal Injury - Med. Malpractice	PERSONAL INJURY <input type="checkbox"/> 365 Personal Injury - Product Liability <input type="checkbox"/> 367 Health Care/Pharmaceutical Personal Injury Product Liability <input type="checkbox"/> 368 Asbestos Personal Injury Product Liability PERSONAL PROPERTY <input type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input type="checkbox"/> 380 Other Personal Property Damage <input type="checkbox"/> 385 Property Damage Product Liability	<input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881 <input type="checkbox"/> 690 Other LABOR <input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Mgmt. Relations <input type="checkbox"/> 740 Railway Labor Act <input type="checkbox"/> 751 Family and Medical Leave Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Empl. Ret. Inc. Security Act IMMIGRATION <input type="checkbox"/> 462 Naturalization Application <input type="checkbox"/> 463 Habeas Corpus - Alien Detainee (Prisoner Petition) <input type="checkbox"/> 465 Other Immigration Actions	<input type="checkbox"/> 422 Appeal 28 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157 PROPERTY RIGHTS <input type="checkbox"/> 820 Copyrights <input type="checkbox"/> 830 Patent <input type="checkbox"/> 840 Trademark SOCIAL SECURITY <input type="checkbox"/> 861 HIA (1395ff) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW (405(g)) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g)) FEDERAL TAX SUITS <input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant) <input type="checkbox"/> 871 IRS—Third Party 26 USC 7609	<input type="checkbox"/> 375 False Claims Act <input type="checkbox"/> 400 State Reapportionment <input type="checkbox"/> 410 Antitrust <input type="checkbox"/> 430 Banks and Banking <input type="checkbox"/> 450 Commerce <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations <input type="checkbox"/> 480 Consumer Credit <input type="checkbox"/> 490 Cable/Sat TV <input type="checkbox"/> 850 Securities/Commodities/Exchange <input type="checkbox"/> 890 Other Statutory Actions <input type="checkbox"/> 891 Agricultural Acts <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 895 Freedom of Information Act <input type="checkbox"/> 896 Arbitration <input type="checkbox"/> 899 Administrative Procedure Act/Review or Appeal of Agency Decision <input type="checkbox"/> 950 Constitutionality of State Statutes
REAL PROPERTY	CIVIL RIGHTS	PRISONER PETITIONS			
<input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property	<input checked="" type="checkbox"/> 440 Other Civil Rights <input type="checkbox"/> 441 Voting <input type="checkbox"/> 442 Employment <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 445 Amer. w/Disabilities - Employment <input type="checkbox"/> 446 Amer. w/Disabilities - Other <input type="checkbox"/> 448 Education	<input type="checkbox"/> 510 Motions to Vacate Sentence Habeas Corpus: <input type="checkbox"/> 530 General <input type="checkbox"/> 535 Death Penalty <input type="checkbox"/> 540 Mandamus & Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Condition <input type="checkbox"/> 560 Civil Detainee - Conditions of Confinement			

V. ORIGIN (Place an "X" in One Box Only)

- 1 Original Proceeding
- 2 Removed from State Court
- 3 Remanded from Appellate Court
- 4 Reinstated or Reopened
- 5 Transferred from another district (specify)
- 6 Multidistrict Litigation

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):
First, Fourth, Fifth and Sixth Amendments; Federal Rule 41(g) return, Property FIS
 Brief description of cause:
Failure to return property + USA policies; unlawful search, abusive prose, culture

VII. REQUESTED IN COMPLAINT:

CHECK IF THIS IS A CLASS ACTION UNDER F.R.C.P. 23

DEMANDS: _____ CHECK YES only if demanded in complaint: culture

JURY DEMAND: Yes No

VIII. RELATED CASE(S) IF ANY

(See instructions): US District Court of Maryland
 JUDGE Richard D. Bennett DOCKET NUMBER Civ. (No. RDB-11-3245)

DATE: 7/25/12 SIGNATURE OF ATTORNEY OF RECORD: Alicia Roark, pro se

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

S. AMANDA MARSHALL, OSB # 95347

United States Attorney

District of Oregon

JAMES E. COX, JR., OSB # 08565

jim.cox@usdoj.gov

Assistant United States Attorney

United States Attorney's Office

District of Oregon

1000 SW Third Ave., Suite 600

Portland, Oregon 97204-2902

Telephone: (503) 727-1026

Facsimile: (503) 727-1117

Attorneys for Defendant United States

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

DIANE ROARK,

Plaintiff,

v.

UNITED STATES OF AMERICA,

Defendant.

Case No.: 6:12-CV-01354-MC

**DEFENDANT'S MOTION FOR
SUMMARY JUDGMENT AND
MEMORANDUM IN SUPPORT**

ORAL ARGUMENT REQUESTED

Defendant the United States of America, by S. Amanda Marshall, United States Attorney for the District of Oregon, and through James E. Cox, Jr., Assistant United States Attorney for the District of Oregon, submits the following motion for summary judgment pursuant to Federal Rule of Procedure 56. This motion is based on the accompanying memorandum in support, the

concurrently-filed declarations of Miriam P., Charles E.¹, Darren M. Dick, Kirsten M. Ruhland and Laura J. Pino, and the exhibits attached thereto, and all pleadings of record herein. Pursuant to Local Rule 7-1, the parties made a good faith effort to resolve this dispute and have been unable to do so.

DATED this 30th day of September 2014.

Respectfully submitted,

S. AMANDA MARSHALL
United States Attorney
District of Oregon

/s/ James E. Cox, Jr.
JAMES E. COX, JR.
Assistant United States Attorney
Attorneys for Defendant

¹ Section 6 of the National Security Agency Act of 1959, 50 U.S.C. § 3605 (Pub. L. No. 86-36) authorizes the National Security Agency (NSA) to protect from public disclosure, among other categories of information, the names of its employees. Miriam P. and Charles E. occupy non-public positions with the NSA. Thus, the names of these NSA employees are referred to by first name, last initial. The Agency is prepared to provide the full name of any employee in an *ex parte*, under seal filing should the Court so require.

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	FACTUAL AND PROCEDURAL BACKGROUND.....	1
A.	Plaintiff’s Employment with HPSCI.....	1
B.	Classified Information and National Security Agency Act (“NSAA”) Information.	4
1.	Classified Information.	4
2.	NSAA Information.	5
C.	The Criminal Investigation into Leaks of Classified Information About the Terrorist Surveillance Program.....	7
D.	The Government Has Returned All Property That Does Not Contain Classified or Protected Information.	8
1.	NSA review for classified and NSAA information.....	8
2.	HPSCI review for HPSCI information.....	10
E.	Procedural History.....	11
1.	The Maryland action.....	11
2.	This action.	13
III.	STANDARD OF REVIEW	14
IV.	ARGUMENT.....	15
A.	The Government Is Entitled To Retain Seized Property in Which It Has a Continuing Interest or Right to Possession.....	15
B.	The Government Is Entitled To Retain the Property Containing Classified Information. 16	
C.	The Government Is Entitled To Retain the Property Containing NSAA information... 18	
D.	The Government is Entitled to Retain the Property Containing HPSCI Information.... 20	
E.	Plaintiff’s Computer Cannot Be Returned Because It Is an Information Storage Media Classified at the TOP SECRET SCI Level.....	21
V.	CONCLUSION.....	23

TABLE OF AUTHORITIES

FEDERAL CASES

<i>Al-Haramain Islamic Found., Inc. v. Bush</i> , 507 F.3d 1190, 1194 (9th Cir. 2007).....	7
<i>Anderson v. Liberty Lobby, Inc.</i> , 477 U.S. 242, 248 (1986).....	14
<i>Berman v. CIA</i> , 501 F.3d 1136, 1140 (9th Cir. 2007).....	19
<i>Bivens v. Six Unknown Named Agents of the Fed. Bureau of Narcotics</i> , 403 U.S. 388 (1971) ...	13
<i>Celotex Corp. v. Catrett</i> , 477 U.S. 317, 322 (1986).....	14
<i>Dept. of Navy v. Egan</i> , 484 U.S. 518, 528 (1988)	4
<i>Gravel v. United States</i> , 408 U.S. 606, 621-22 n. 13 (1972).....	21
<i>Hayden v. Nat’l Sec. Agency/Central Sec. Serv.</i> , 608 F.2d 1381, 1391 (D.C. Cir. 1979)	19
<i>Kardoh v. United States</i> , 572 F.3d 697, 700 (9th Cir. 2009).....	15
<i>Lahr v. Nat’l Transpo. Safety Bd.</i> , 569 F.3d 964, 985 (9th Cir. 2009).....	6, 18, 19
<i>Minier v. C.I.A.</i> , 88 F.3d 796, 800 (9th Cir. 1996)	19
<i>United States v. Fitzen</i> , 80 F.3d 387, 388 (9th Cir. 1996)	16
<i>United States v. Ibrahim</i> , 522 F.3d 1003, 1008 (9th Cir. 2008)	15
<i>United States v. Martinson</i> , 809 F.2d 1364, 1369 (9th Cir. 1987).....	16
<i>United States v. Van Cauwenberghe</i> , 934 F.2d 1048, 1060-61 (9th Cir. 1991).....	15
<i>Weinberger v. Catholic Action of Hawaii/Peace Educ. Project</i> , 454 U.S. 139, 145-46 (1981)...	17
<i>Wiebe v. National Sec. Agency</i> , Civil Action No. RDB–11–3245, 2012 WL 1670046 (D. Md. May 11, 2012).....	12
<i>Wiebe v. National Sec. Agency</i> , Civil Action No. RDB–11–3245, 2012 WL 4069746 (D. Md. Sept. 14, 2012)	passim

FEDERAL STATUTES

18 U.S.C. § 798.....	17
5 U.S.C. § 552(b)(1)	17
50 U.S.C. § 1803.....	7
50 U.S.C. § 3161(a)	16
50 U.S.C. § 3605.....	6, 19, 20

FEDERAL RULES

Fed. R. Civ. P. 56(a) 14
Fed. R. Civ. P. 56(c) 14
Fed. R. Civ. P. 56(e) 14

FEDERAL REGULATIONS

28 C.F.R. § 17.18(a)..... 5

OTHER AUTHORITIES

Exec. Order No. 13470, 73 Fed. Reg. 45325 (July 30, 2008)..... 6
Exec. Order No. 13526, 75 Fed. Reg. 707 (Jan. 5, 2010)..... 4, 17
Rules of the House of Representatives, 113th Cong. (2013)..... 2, 3, 17
Rules of the Permanent Select Comm. on Intelligence, U.S. House of Representatives, 106th
Cong. (1999) 2, 3, 17, 20
Rules of the Permanent Select Comm. on Intelligence, U.S. House of Representatives, 113th
Cong. (2013) 3, 20

MEMORANDUM IN SUPPORT

I. INTRODUCTION

This case is a motion for the return of property seized by the government as part of a criminal investigation into a leak of classified information. Plaintiff Diane Roark (“Plaintiff”) is a retired staff employee of the House Permanent Select Committee on Intelligence (“HPSCI”) who lives in Stayton, Oregon. The government conducted a lawful search of Plaintiff’s residence in July 2007 pursuant to a search warrant and seized various items – primarily documents referencing National Security Agency intelligence programs. The criminal investigation has concluded and the government has returned much of the property that was seized from Plaintiff in the July 2007 search.

The only seized property that the government has not agreed to return to Plaintiff are 28 documents/notebooks, one compact disc (CD), and one desktop computer. The government has not returned the foregoing property because it contains information that is either classified, protected by the National Security Agency Act of 1959, and/or protected by the non-disclosure agreements signed by Plaintiff. The government has a continuing interest in ensuring that such information is not publicly disclosed. This interest is sufficient to justify the government’s retention of the property. For this reason, Plaintiff’s motion for return of property should be denied.

II. FACTUAL AND PROCEDURAL BACKGROUND

A. Plaintiff’s Employment with HPSCI.

Plaintiff Diane Roark (“Plaintiff”) worked on the staff of the House Permanent Select Committee on Intelligence (“HPSCI”) from 1985 to 2002. HPSCI is the committee to which the House refers “proposed legislation, messages, petitions, memorials, and other matters” relating to the “Central Intelligence Agency, the Director of National Intelligence, [] the National

Intelligence Program” and the “[i]ntelligence and intelligence-related activities of all other departments and agencies of the Government.” Rule X.11(b)(1), Rules of the House of Representatives, 113th Cong. (2013) (“House Rules”), *available online* <http://clerk.house.gov/legislative/house-rules.pdf>. HPSCI is also responsible for “review and study on a continuing basis laws, programs, and activities of the intelligence community and shall review and study on an exclusive basis the sources and methods of [certain intelligence agencies].” House Rule X.3(m).

In the course of performing their jobs, HPSCI staff members are privy to sensitive national security information. (Declaration of Darren M. Dick (“Dick Decl.” ¶ 3.) Certain restrictions apply to HPSCI staff in dealing with such information. HPSCI rules in force during Ms. Roark’s employment stated that HPSCI staff “shall not . . . discuss or disclose:

- (A) the classified substance of the work of the Committee;
- (B) any information received by the Committee in executive session;²
- (C) any classified information received by the Committee from any source; or
- (D) the substance of any hearing that was closed to the public pursuant to these rules or the Rules of the House.”

(Dick Decl., Ex. 1 at p. 8 (Rule 12(a)(1), 1999 Committee Rules); *id.* at p. 10, Rule 13(b) (“Any classified information received by the Committee, from any source, shall not be disclosed”).) This prohibition applies during a staff member’s “tenure as a member of the Committee or as Committee Staff, or anytime thereafter.” (*Id.* at p. 8, Rule 12(a)(1).) Nearly identical rules remain in force today. (*Id.*, Ex. 2 at pp. 8-9, Rule 12(a)(1), Rules of the Permanent Select

² An “executive session” is a committee meeting or hearing that is closed to the public. Committee meetings may be closed if disclosure of the matters to be discussed may “endanger national security” or “compromise sensitive law enforcement information.” (Dick Decl., Ex. 1 at p. 3 (Rule 5(b), Rules of the Permanent Select Comm. on Intelligence, U.S. House of Representatives, 106th Cong. (1999) (“1999 Committee Rules”); *see also* House Rule XI.2(g)(1) (authorizing committees to conduct meetings in executive session).

Comm. on Intelligence, U.S. House of Representatives, 113th Cong. (2013) (“2013 Committee Rules”).)

Furthermore, HPSCI staff members are required to sign a non-disclosure agreement (“NDA”) before joining the committee staff in which they promise “not to divulge any classified information which comes into [their] possession while a member of the Committee Staff” except in authorized circumstances. (*Id.*, Ex. 1 at p. 9, Rule 12(b)(1) of 1999 Committee Rules; House Rules X.11(e) (stating that HPSCI employees may not have access to classified information unless they agree in writing to follow House and committee rules “concerning the security of classified information during and after the period of the[ir] employment”).)

Plaintiff signed NDAs with HPSCI at the beginning of her employment in 1985 and again in 1999. (Dick Decl. Exs. 3, 4.) In executing the NDA, Plaintiff agreed to be bound by the rules of the House and the HPSCI Rules of Procedure. (*Id.*, Ex. 4 at ¶ 7.) By those NDAs, Plaintiff further agreed she would “never divulge, publish, or reveal by writing, word, conduct, or otherwise, either during [her] tenure with the HPSCI or anytime thereafter” any:

- “[T]estimony given before the HPSCI in executive session, including the names of any witness who appeared before the HPSCI in executive session,”
- “Material, restricted data, . . . or information received or generated by the HPSCI that has been identified under established HPSCI security procedures, by Executive Order, by the Director of Central Intelligence (DCI), or otherwise by statute, as requiring protection from unauthorized disclosure,” and
- “Any information classified pursuant to any Executive Order, by the DCI, or otherwise by statute, which might otherwise come into [her] possession.”

(*Id.* at ¶¶ 2, 13.) Ms. Roark also agreed that she would “surrender to the HPSCI . . . upon [her] separation from the HPSCI staff” all “information, material, or restricted data” in the foregoing categories. (*Id.* at ¶ 7.)

B. Classified Information and National Security Agency Act (“NSAA”) Information.**1. Classified Information.**

“Since World War I, the Executive Branch has engaged in efforts to protect national security information by means of a classification system graded according to sensitivity.” *Dept. of Navy v. Egan*, 484 U.S. 518, 528 (1988). By executive order, the President has established “a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism.” Exec. Order No. 13526, Part 1, Sec. 1.2(a), 75 Fed. Reg. 707 (Jan. 5, 2010).

Certain prerequisites must be met for information to be deemed classified. Most importantly, an original classification authority must “determine[] that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security.” *Id.* at Sec. 1.1(a)(4). Furthermore, classified information must be “owned by, produced by or for, or [be] under the control of the United States Government.” *Id.* at Sec. 1.1(a)(2). In addition, classified information must pertain to one of eight topics, one of which is “intelligence activities (including covert action), intelligence sources or methods, or cryptology.” *Id.* at Sec. 1.4.

An original classification authority can classify information at any of three levels – Confidential, Secret and Top Secret. *Id.* at Sec. 1.2. The classification level is based on the amount of damage to national security that reasonably could be expected to occur based on unauthorized disclosure of the information. *Id.* Unauthorized disclosure of Confidential information could reasonably be expected to cause damage to national security, unauthorized disclosure of Secret information could reasonably be expected to cause serious damage to national security, while unauthorized disclosure of Top Secret information could reasonably be expected to cause exceptionally grave damage to national security. *Id.*

Classified information can also receive an additional designation of “sensitive compartmented information” (or “SCI”) if it “not only is classified for national security reasons as Top Secret, Secret, or Confidential, but also is subject to special access and handling requirements because it involves or derives from particularly sensitive intelligence sources and methods.” 28 C.F.R. § 17.18(a). One subcategory of SCI is “SI,” a marking used to protect certain Communications Intelligence. (Declaration of Miriam P. (“Miriam P. Decl.”) ¶ 7.) Communications Intelligence is SCI that was derived from exploiting cryptographic systems or other protected sources by applying methods or techniques, or from intercepted foreign communications. (*Id.*)

Because of the exceptional sensitivity and vulnerability of SCI, the government utilizes safeguards and access requirements that exceed the access standards that are normally required for information of the same classification level. (*Id.*) Less than one year before her retirement from HPSCI, Roark signed an additional NDA regarding her obligations with respect to SCI. (Exhibit 1, attached hereto.) That NDA includes provisions in which Plaintiff:

- agreed not to divulge SCI (¶ 3);
- agreed to submit for security review any writings that contain or purport to contain any SCI or description of activities that produce or relate to SCI (¶ 4);
- agreed to return all materials containing SCI at the conclusion of her employment (¶ 8);
- stipulated that all information to which she obtains access by signing the Agreement will remain the property of the United States Government unless and until otherwise determined by an appropriate official or final ruling of a court of law. (¶ 8.)

(*Id.*) The conditions and obligations imposed by the NDA applied during the time Plaintiff was granted access to SCT, “and at all times thereafter.” (*Id.* at ¶ 9.)

2. NSAA Information.

The National Security Agency (“NSA”) is a government agency responsible for “collect[ing] (including through clandestine means), process[ing], analyz[ing], produc[ing] and

disseminat[ing] signals intelligence information and data for foreign intelligence and counterintelligence purposes” and for “establish[ing] and operat[ing] an “effective unified organization for signals intelligence activities.” *See* Exec. Order No. 13470, at Sec. 1.7(c)(2), 73 Fed. Reg. 45325, 45335 (July 30, 2008). In performing its signals intelligence mission, NSA exploits foreign signals to obtain intelligence information necessary to the national defense, national security, or the conduct of foreign affairs. (Miriam P. Decl., ¶ 5.) NSA has developed a sophisticated worldwide signals intelligence collection network that acquires, among other things, foreign and international electronic communications. (*Id.*) The technological infrastructure that supports the NSA’s foreign intelligence information collection network has taken years to develop at a cost of billions of dollars and untold human effort. (*Id.*) It relies on sophisticated collection and processing technology. (*Id.*)

Congress has specifically recognized the inherent sensitivity of the activities of the NSA by enacting laws to protect the fragile nature of the NSA’s signals intelligence efforts. (*Id.* at ¶ 14.) One of these laws is a statutory privilege specific to the NSA. (*Id.*) The NSA’s statutory privilege is set forth in section 6 of the National Security Agency Act of 1959, Public Law 86-36, 50 U.S.C. § 3605. (*Id.*) Section 6 of the NSA Act provides that “[n]othing in this Act or any other law . . . shall be construed to require the disclosure of the organization or any function of the National Security Agency, or any information with respect to the activities thereof, or of the names, titles, salaries, or number of the persons employed by such agency.” 50 U.S.C. § 3605. Information need not be classified to fall within the purview of 50 U.S.C. § 3605, and such information (hereinafter “NSAA information”) is exempt from disclosure under the Freedom of Information Act (“FOIA”). *See Lahr v. Nat’l Transpo. Safety Bd.*, 569 F.3d 964, 985 (9th Cir. 2009).

C. The Criminal Investigation into Leaks of Classified Information About the Terrorist Surveillance Program.

Following the September 11, 2001 attacks on the United States, President George W. Bush established the Terrorist Surveillance Program (“TSP”), authorizing the NSA to intercept international communications into and out of the United States of persons linked to al Qaeda or related terrorist organizations. (Declaration of Laura Pino (“Pino Decl.”), Ex. 1 at ¶ 7.)³ On December 15, 2005, the New York Times began publishing a series of articles describing a range of alleged NSA activities, including the TSP. (*Id.* at ¶ 9.) Shortly after the first TSP article, the Department of Justice and the FBI initiated an investigation concerning the unauthorized disclosure of classified information contained in that article. (*Id.* at ¶ 12.) That investigation involved interviews of in excess of 1,000 individuals, issuance of more than 200 grand jury subpoenas, principally for telephone and email records, and review of thousands of pages of documents, including telephone and email records for approximately 60 individuals. (*Id.*) Through that process, among the individuals identified as subjects of the investigation were Roark and four former employees of the NSA – William Binney (“Binney”), Thomas Drake (“Drake”), Edward Loomis (“Loomis”), and John Wiebe (“Wiebe”). (*Id.* at ¶ 13.)

In July 2007, the government applied for and obtained warrants to search the homes of Binney, Loomis, Wiebe, and Roark for evidence related to the criminal investigation. (*Id.* at ¶ 53.) On July 26, 2007, the FBI executed the search warrants. The FBI seized a variety of items in Roark’s possession, including a desktop computer, a cell phone, a fax machine, and a

³ In January 2007, the Attorney General announced that any electronic surveillance that was occurring under the TSP would henceforth be conducted subject to the approval of the Foreign Intelligence Surveillance Court, *see* 50 U.S.C. § 1803, and that the President’s authorization of the TSP had lapsed. *See, e.g., Al-Haramain Islamic Found., Inc. v. Bush*, 507 F.3d 1190, 1194 (9th Cir. 2007).

number of papers, folders, and notebooks. (*Id.* at Ex. 2.) A lawful search was also conducted later in the year on Drake's residence.

No criminal charges were filed against Binney, Loomis, Wiebe, or Roark as a result of the investigation. A criminal case initiated against Drake in the District of Maryland resulted in a guilty plea to a misdemeanor charge of exceeding authorized use of a computer and dismissal of felony charges. *See United States v. Drake*, District of Maryland, Case No. 1:10-cr-181-RDB.

D. The Government Has Returned All Property That Does Not Contain Classified or Protected Information.

The FBI has returned all of the seized property that does not contain classified information, NSAA information, and/or information protected by Plaintiff's NDA with HPSCI ("HPSCI information"). (Pino Decl., ¶ 4; Miriam P. Decl., ¶¶ 12, 15; Dick Decl., ¶ 8.) The property that the FBI has not returned to Plaintiff consists of 28 paper documents/notebooks, one CD, and one desktop computer. (Pino Decl., Ex. 3.)

1. NSA review for classified and NSAA information.

Miriam P., the Deputy Chief of Staff for Policy and Corporate Issues for the Signals Intelligence Directorate of the NSA and an original classification authority, has performed a classification review of some of the items retained by the government from the 2007 search and seizure. (Miriam P. Decl., ¶ 11.) Based on this review, Miriam P. has determined that four of the paper documents that the government retains contain information properly classified at the SECRET level. (*Id.* at ¶ 12.) These four documents include three copies of a four page document Plaintiff submitted to the NSA for permission to publish, and one 18 page set of Commander Naval Security Group slides. (*Id.*)

The category of classified information to which the four documents listed above pertain is intelligence activities (including covert action), intelligence sources and methods, or cryptology. (*Id.* at ¶ 13.) Disclosure of the classified information in these documents reasonably could be expected to cause serious damage to United States national security by compromising SIGINT intelligence sources, methods and/or activities. (*Id.*)

Specifically, the 18-page set of slides contains Electronic Intelligence (ELINT) information. (*Id.*) Electronic Intelligence, a subset of Signals Intelligence, is technical and intelligence information derived from foreign non-communications electronic signals, such as radars and radar-jamming signals. (*Id.*) The three copies of the four page document contain Communications Intelligence (COMINT) information, which is technical and intelligence information derived from foreign communications signals and data. (*Id.*) This COMINT information is also Sensitive Compartmented Information (SCI). (*Id.*, ¶¶ 7, 13.)⁴

Miriam P. has also concluded that another 18 of the paper documents/notebooks that the government still retains from the search and seizure contain NSAA information, as does the one CD. (*Id.*, ¶¶ 15.) These items contain the names and/or contact information for NSA employees. (*Id.* ¶ 16.)⁵

Finally, the NSA has also analyzed the hard drive on the desktop computer drive seized from Plaintiff's residence to identify whether any classified information or NSAA information was present. (Declaration of Charles E. ("Charles E. Decl."), ¶ 3.) To perform this analysis,

⁴ In addition to the four paper documents that the NSA determined contain classified information, the U.S. Navy has determined that another paper document also contains classified information. (Declaration of Kirsten M. Ruhland, ¶¶ 1-2.) Thus, five of the paper documents have been deemed to include classified information.

⁵ Due to the length of some of these documents and the difficulty in reading some of the handwritten notes, Miriam P. only confirmed the presence of NSAA information in at least one location of each item. (*Id.*, ¶¶ 15 n. 2.) Thus, it is possible these items may also contain classified information. (*Id.*)

Charles E. – a computer forensic examiner with the NSA – performed an initial search of data in Plaintiff’s user profile directory using a set of search terms designed to identify potentially classified or NSAA information. (*Id.* at ¶¶ 3, 4.) This initial search was only conducted of the user profile directory and did not include other directories, such as the directories that appear to include more than 10,000 America On-Line (AOL) emails. (*Id.* at ¶ 3.) Charles E. identified 53 files that were responsive to the search terms, and provided four of the potentially classified items to Miriam P. for review. (*Id.* at ¶ 4.) Miriam P. determined that the four files included information that is properly classified as “TOP SECRET” (Miriam P. Decl. at ¶ 17.) The classified information on Plaintiff’s computer was information that involves intelligence activities (including covert action), intelligence sources and methods, or cryptology. (*Id.* at ¶ 18.) Disclosure of the classified information reasonably could be expected to cause exceptionally grave damage to United States national security by compromising SIGINT intelligence sources, methods and/or activities. All four files contain Communications Intelligence information, which is Sensitive Compartment Information (SCI). (*Id.* at ¶¶ 17-18.)

2. HPSCI review for HPSCI information.

Darren M. Dick, the Staff Director of the HPSCI, has also reviewed some of the information retained by the government to determine whether any of the documents contain HPSCI information (i.e., testimony given before HPSCI in executive session, information received or generated by HPSCI that has been identified as requiring protection from unauthorized disclosure (under established HPSCI security procedures, by Executive Order, by the Director of Central Intelligence, or otherwise by statute), or classified information). (Dick Decl., ¶ 8, *see also id.*, Ex. 4.) Based on this review, Mr. Dick determined that 16 of the items

the government retains from the 2007 search contain HPSCI information. (*Id.* at ¶ 8.)⁶ Of those 16 items:

- Five are protected because they include information received or generated in HPSCI executive-session,
- Six are protected because they contain information that has been identified under established HPSCI security procedures, by Executive Order, by the Director of Central Intelligence, or otherwise by statute as requiring protection from disclosure, and
- Five are protected they include information received or generated in HPSCI executive-session *and* because they contain information that has been identified as requiring protection from disclosure. (*Id.*)⁷

Furthermore, at least six of the items existed prior to Plaintiff's retirement from HPSCI and therefore should have been surrendered to HPSCI at that time pursuant to paragraph 7 of Plaintiff's non-disclosure agreement. (*Id.* at ¶¶ 8, 9.)

E. Procedural History.

1. The Maryland action.

In November 2011, Wiebe filed a motion in the U.S. District Court for the District of Maryland under Federal Rule of Criminal Procedure 41(g) for the return of his property seized in the July 2007 search of his residence. *See Wiebe v. Nat'l Security Agency, et al.*, District of Maryland Case No. 1:11-cv-3245 (hereinafter, "the Maryland Action"). Binney, Loomis, Roark and Drake each filed motions to consolidate in which they requested return of the property seized during the searches of their residences. The government moved to dismiss Roark from the Maryland Action for improper venue because the search of her property occurred in Oregon

⁶ These 16 items include some items that are also subject to a claim of protection by the NSA. Exhibit 3 to the Declaration of Laura J. Pino is a chart that sets forth the items that have not been returned and the claims asserted for those items. The chart also includes nine items that were recently returned to Plaintiff or are in the process of being returned. The government notes that the document labeled "HC38" was sent by the FBI to undersigned counsel today and counsel will forward it to Plaintiff immediately upon receipt.

⁷ The Navy completed its classification review of document "HC3" after Mr. Dick executed his declaration. Based on the Navy's review of HC3, HPSCI would likely view that document as "requiring protection from disclosure" as well, which would raise to six the number of items that are protected under both HPSCI grounds.

pursuant to a subpoena issued in the District of Oregon. The Maryland court granted the motion and dismissed Roark from the case. *See Wiebe v. National Sec. Agency*, Civil Action No. RDB–11–3245, 2012 WL 1670046 (D. Md. May 11, 2012)

Following Roark’s dismissal from the litigation, the parties filed dispositive motions on the claims of the remaining petitioners in the Maryland Action. The government claimed that certain property need not be returned because it contained (1) classified information, (2) NSAA information, or (3) government information controlled by other government agencies (“OGA information”). The district court granted the government’s motion in relevant part. (Exhibits 2, 3 attached hereto, *Wiebe v. National Sec. Agency*, Civil Action No. RDB–11–3245, 2012 WL 4069746 (D. Md. Sept. 14, 2012); *recommendation aff’d* docket # 78 (D. Md. Mar. 27, 2013).)⁸

Specifically, the Maryland court ruled that the government’s determination that seized documents contained classified or NSAA information was not subject to judicial review and that the presence of such information in any seized property was a sufficient ground for the government to retain such property. *Id.* at * 3-6. The Court held that the government also has a continuing interest in OGA information; however, the evidentiary record was not sufficient to establish whether the government was entitled to retain the property labeled as OGA information. *Id.* at *9.

The Maryland court also noted that petitioners’ argument that the searches were unlawful was irrelevant. The court observed that Fed. R. Cr. P. 41(g) “provides a remedy to petitioners who have been aggrieved by an unlawful search and seizure *or* by a deprivation of property.” *Id.* at *9 (emphasis in original). Since the petitioners had “already established a deprivation of property, . . . establishing an unlawful search or seizure [was] unnecessary.” *Id.* Thus, the only

⁸ The government requests that the Court take judicial notice of any pleadings and orders issued in the Maryland Action pursuant to Federal Rule of Evidence 201.

remaining issue was whether the government “has a continuing interest in the classified, NSAA, and OGA information, and establishing a Fourth Amendment violation would not diminish or vitiate this interest.” *Id.*

Following the summary judgment ruling, the Maryland Court allowed the petitioners to accept the government’s offer to return any unprotected information on the petitioners’ computer that the petitioners wished to be reviewed for return. *Id.* at *10. That process has been completed for petitioners Wiebe, Binney and Loomis, and is nearing completion for petitioner Drake.

2. This action.

On July 26, 2012, Roark filed her complaint in this action. As she did in the Maryland Action, Plaintiff “seeks return of her remaining property, except those items that she has said need not be returned.” (Docket (“Dkt.”) # 1, Complaint at ¶ 14.) Plaintiff sought this relief, though, “only if necessary under an associated Rule 41(g) action following resolution of constitutional issues.” (*Id.*) The “constitutional issues” involved requests for declaratory and injunctive relief and damages. (*Id.* at ¶¶ 11-13.)

The government moved to dismiss all claims except the return of property claim on the ground that plaintiff lacked standing and the Court lacked jurisdiction. (Dkt. # 8.) Plaintiff subsequently moved to amend her complaint to add constitutional claims for damages under *Bivens v. Six Unknown Named Agents of the Fed. Bureau of Narcotics*, 403 U.S. 388 (1971). (Dkt. # 18.) Plaintiff also requested dismissal of her constitutional claims if the Court denied the motion for leave to amend. (*Id.* at p. 4 (“Should the Court refuse to approve this amended complaint, Plaintiff requests a voluntary dismissal of the constitutional aspects of her lawsuit without prejudice, and a continuance of the Rule 41 (g) return of property lawsuit.”).)

This Court denied Plaintiff's motion for leave to amend on the grounds that the proposed *Bivens* claims were barred by the statute of limitations and failed to state a claim for relief. (Dkt # 35.) The Court granted Plaintiff's request to voluntarily withdraw the constitutional claims in the case, "leaving for litigation a Fed. R. Crim. P. 41(g) lawsuit for return of property." (*Id.* at p. 14.)

III. STANDARD OF REVIEW

Pursuant to Fed. R. Civ. P. 56, "[a] party may move for summary judgment, identifying each claim or defense — or the part of each claim or defense — on which summary judgment is sought." Fed. R. Civ. P. 56(a). Summary judgment is appropriate where the evidence "shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." *Id.*; *see Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986).

Materiality of a fact is determined from the substantive law governing the claim. *See Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). Disputes over facts that might affect the outcome of the lawsuit according to applicable substantive law are "material." *Id.* A dispute concerning a material fact is "genuine" if the evidence is sufficient to allow a reasonable jury to return a verdict for the nonmoving party. *Id.* at 248-49. The substantive law distinguishes critical facts from irrelevant facts, and only disputes over facts that might affect the outcome will preclude summary judgment. *Id.* at 248. The moving party bears the burden to establish the absence of a genuine issue of material fact and that it is entitled to judgment as a matter of law. Fed. R. Civ. P. 56(c); *Anderson*, 477 U.S. at 247; *Celotex*, 477 U.S. at 323. Once the moving party meets this burden, the nonmoving party may not rest on the allegations of the pleadings but must by affidavit or other evidence set forth specific facts that show a genuine issue of material fact exists. Fed. R. Civ. P. 56(e); *Anderson*, 477 U.S. at 256.

IV. ARGUMENT

The FBI has returned most of the property that was seized from Plaintiff's residence during the July 25, 2007 search. The remaining items that have not been returned – 28 paper documents/notebooks, one CD, and a computer hard drive – all contain classified information, information protected under the National Security Agency Act of 1959, ("NSAA information"), and/or information protected by HPSCI in its non-disclosure agreement with Plaintiff ("HPSCI information"). The government has a continuing interest in this information that justifies its retention of this information. Thus, Plaintiff's motion for return of property should be denied.

A. **The Government Is Entitled To Retain Seized Property in Which It Has a Continuing Interest or Right to Possession.**

Federal Rule of Criminal Procedure 41(g) provides as follows:

Motion to Return Property. A person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return. The motion must be filed in the district where the property was seized. The court must receive evidence on any factual issue necessary to decide the motion. If it grants the motion, the court must return the property to the movant, but may impose reasonable conditions to protect access to the property and its use in later proceedings.

"Where no criminal proceeding is pending, a district court has discretion to hear a motion for the return of property as a civil equitable proceeding." *See Kardoh v. United States*, 572 F.3d 697, 700 (9th Cir. 2009). Once a Rule 41(g) motion is treated as a civil complaint, the district court is "required to apply the Federal Rules of Civil Procedure." *United States v. Ibrahim*, 522 F.3d 1003, 1008 (9th Cir. 2008).

"Ordinarily, property seized for purposes of a trial that is neither contraband nor subject to a forfeiture statute is to be returned to the defendant at the end of the trial." *United States v. Van Cauwenberghe*, 934 F.2d 1048, 1060-61 (9th Cir. 1991). "[W]hen the property in question is no longer needed for evidentiary purposes, either because trial is complete, the defendant has

pleaded guilty, or [] the government has abandoned its investigation, the burden of proof changes.” *United States v. Martinson*, 809 F.2d 1364, 1369 (9th Cir. 1987). “The person from whom the property is seized is presumed to have a right to its return, and the government has the burden of demonstrating that it has a legitimate reason to retain the property.” *Id.* “The government, however, may overcome this presumption by demonstrating a cognizable claim of ownership or right to possession adverse to that of [the defendant].” *United States v. Fitzen*, 80 F.3d 387, 388 (9th Cir. 1996) (internal quotations omitted); *Wiebe*, 2012 WL 4069746 at *5 (“Pursuant to Rule 41(g), courts must determine if the government’s retention of seized property is ‘reasonable,’ and must balance the government’s need to retain the property against the individual’s right to use the property.”)

B. The Government Is Entitled To Retain the Property Containing Classified Information.

The government has a continuing interest in classified information, regardless of where it is located or who possesses it. This interest is demonstrated by the numerous laws and regulations restricting access to and disclosure of classified information, and the promises required of and made by executive and congressional employees (including Plaintiff) who handle classified information.

With respect to access to classified information, the President is required by law to “establish procedures to govern access to classified information which shall be binding upon all departments, agencies, and offices of the executive branch of Government.” 50 U.S.C. § 3161(a). Pursuant to this authority, the President has mandated that a person may only receive access to classified information if an agency has determined that the person is eligible, the person has signed a non-disclosure agreement, and the person needs to know the information. Exec.

Order No. 13526, at Part 1, Sec. 4.1(a). Congress has enacted similar restrictions for its employees. *See* House Rule XXIII.13; Dick Decl., Ex. 2 (Rule 14 of 1999 Committee Rules).

Furthermore, the government's interest in classified information is also demonstrated by the restrictions it places on disclosure of classified information. "Classified information may not be removed from official premises without proper authorization," and an "employee leaving agency service may not remove classified information from the agency's control." Exec. Order No. 13526, at Part 1, Sec. 4.1; *see also* Dick Decl., Ex. 2 (Rules 12, 13 of 1999 Committee Rules). Likewise, classified information is protected from disclosure under the first exemption of the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552(b)(1). *See Weinberger v. Catholic Action of Hawaii/Peace Educ. Project*, 454 U.S. 139, 145-46 (1981). And, under certain circumstances, the unauthorized disclosure of classified information is a crime. 18 U.S.C. § 798.

The government's interest in classified information is also demonstrated by the non-disclosure agreements the government required Plaintiff to execute as a condition for providing access to classified information. Plaintiff acknowledged that she "understand[s] that all information to which I may obtain access by signing this Agreement is now and will remain the property of the United States Government unless and until otherwise determined by an appropriate official or final ruling of a court of law." (Exhibit 1; *see also* Dick. Decl., Ex. 3, 4.)

The government's continuing interest in classified information warrants denial of Plaintiff's claim for return of the documents that contain classified information. The classified information in the documents and computer files seized from Plaintiff involves intelligence activities (including covert action), intelligence sources and methods, or cryptology. (Miriam P Decl. at ¶¶ 12-13, 19-20.) Most of the classified documents contain Communications Intelligence information that is protected within special intelligence (SI), which is a form of

Secure Compartmented Information (SCI). (*Id.*, ¶¶ 7, 13.) Disclosure of the classified information in these documents reasonably could be expected to cause serious or exceptionally grave damage to United States national security by compromising SIGINT intelligence sources, methods and/or activities. (*Id.*)

Plaintiff has acknowledged the government’s ownership interest in SCI in the non-disclosure agreements she signed. (Ex. 1, ¶ 8; Dick Decl., Exs. 3, 4, ¶¶ 7, 10.) In addition, at least six of the paper documents predate the end of Plaintiff’s employment with HPSCI and, thus, her possession of them violates the terms of the non-disclosure agreements. (Ex. 1, ¶ 8 (“I agree that I shall return all materials that have come into my possession or upon the conclusion of my employment or other relationship with the United States Government entity providing me access to such materials.”); Dick Decl., Ex. 4, ¶ 7 (“I hereby agree to surrender . . . upon my separation from the HPSCI staff, all information, material, or restricted data . . .”))

In the return of property case in the district of Maryland that arose from the same criminal investigation, the district court concluded that “[t]he Government has established as a matter of law that the information it deems to be classified or NSAA information . . . cannot be returned to Petitioners.” *See Wiebe*, 2012 WL 4069746 at *9. The Maryland court’s conclusion was correct, and this Court should reach the same conclusion.

C. The Government Is Entitled To Retain the Property Containing NSAA information.

The reasons that the government has a continuing interest in classified information apply equally to unclassified NSAA information. *See Wiebe*, 2012 WL 4069746 at *6. When the NSA declines to disclose NSAA information, “[t]he agency need not make a ‘specific showing of potential harm to national security’ because ‘Congress has already, in enacting the statute, decided that disclosure of NSA activities is potentially harmful.’” *Lahr*, 569 F.3d 964, 985 (9th Cir. 2009) (*quoting Hayden v. Nat’l Sec. Agency/Central Sec. Serv.*, 608 F.2d 1381, 1391 (D.C.

Cir. 1979)); *Berman v. CIA*, 501 F.3d 1136, 1140 (9th Cir. 2007) (noting that the NSAA provides intelligence agencies with a “near-blanket” FOIA exemption).

Nineteen of the items that the government still retains from the 2007 search contain the names and/or contact information for NSA employees. (Miriam P. Decl. at ¶¶ 15-16.) Such information is specifically protected by the NSAA. *See* 50 U.S.C. § 3605 (“Nothing in this Act or any other law . . . shall be construed to require the disclosure of . . . the names, titles, salaries, or number of the persons employed by such agency.”)

The government’s continuing interest in NSAA information justifies the government’s retention of such information. *See Wiebe*, 2012 WL 4069746 at *6; *see also Berman*, 501 F.3d at 1140 (upholding government withholding of NSAA information in FOIA litigation); *Lahr*, 569 F.3d at 985 (same). Plaintiff has acknowledged the government’s interest in NSAA information in the NDA she signed with HPSCI. (Dick Decl., Ex. 4 at ¶ 2 (“I will never divulge, publish, or reveal by writing . . . information received or generated by HPSCI that has been identified . . . by statute, as requiring protection from unauthorized disclosure . . .”).)

The Ninth Circuit’s decision in *Minier v. C.I.A.*, 88 F.3d 796, 800 (9th Cir. 1996), demonstrates the government’s interest in the property at issue here. In *Minier*, the CIA denied the plaintiff’s FOIA request to disclose whether the CIA previously had an employment relationship with a certain individual. The Ninth Circuit held that the CIA’s denial was appropriate under FOIA Exemption 3 because “the plain language of [50 U.S.C.] §§ 403–3(c)(5) and 403g expressly provides that the CIA is exempted from disclosing the names of its employees.” *Id.* at 801. Likewise, the NSAA information in the documents retained from the 2007 search and seizure is unquestionably information that is protected under the plain language

of 50 U.S.C. § 3605. As such, Plaintiff's claim for return of property containing such information should be denied.

D. The Government is Entitled to Retain the Property Containing HPSCI Information.

Congress also has a continuing interest in ensuring the confidentiality of classified and protected information utilized and generated by its members and staff. This is reflected in the steps Congress has taken to protect such information, include enacting rules regarding confidentiality and requiring that staff sign non-disclosure agreements.

HPSCI rules prohibit the unauthorized disclosure of: the classified substance of the work of HPSCI, any information received by HPSCI in executive session, any classified information received by HPSCI, and the substance of any hearing that was closed to the public. (Dick Decl., Ex. 2 (1999 Committee Rule 12(a)(1)); *see also id.* Ex. 3 (2013 Committee Rule 12(a)(1) (same)).)

HPSCI staffers (including Plaintiff) acknowledge the foregoing confidentiality requirements by executing non-disclosure agreements. In her non-disclosure agreement, Plaintiff agreed “never to divulge, publish, or reveal by writing, word, conduct, or otherwise, either during [her] tenure with the HPSCI or anytime thereafter . . . any testimony given before the HPSCI in executive session, including the name of any witness who appeared or was called to appear before the HPSCI in executive session.” (Dick Decl., Ex. 4 at ¶ 2.) She also agreed not to disclose any “material, restricted data, . . . or information received or generated by the HPSCI that has been identified under established HPSCI security procedures, by Executive Order, by the Director of Central Intelligence (DCI), or otherwise by statute, as requiring protection from unauthorized disclosure” (*Id.*) That category included not just classified information, but also information marked “For Official Use Only,” based on the Director of Central Intelligence’s determination that information required protection from unauthorized disclosure. (*Id.* at ¶ 7.)

She further “agree[d] to surrender to the HPSCI . . . upon [her] separation from the HPSCI staff” all material containing such testimony or information. (*Id.*, Ex. 4 at ¶ 7.)

Fifteen of the paper documents and the one compact disc that the government retains from the 2007 search contain information implicated by the foregoing promises. (Dick Decl. ¶ 8.) Furthermore, at least five of the documents and the compact disc are items that existed prior to Plaintiff’s retirement from HPSCI and therefore should have been surrendered to HPSCI at that time pursuant to paragraph 7 of Plaintiff’s non-disclosure agreement. (*Id.* at ¶¶ 8, 9.)

Plaintiff is not entitled to the return of these documents. Under the terms of HPSCI Rules and the non-disclosure agreement Plaintiff signed, this property contains confidential information which belongs to HPSCI. (Dick Decl., Ex. 2; *id.* at Ex. 4, ¶¶ 2, 7.)⁹

E. Plaintiff’s Computer Cannot Be Returned Because It Is an Information Storage Media Classified at the TOP SECRET SCI Level.

As noted earlier, *supra* part II.D.1., Plaintiff’s computer hard drive contains at least four files that include classified information. (Miriam P. Decl., ¶ 17.) According to NSA Policy, an information storage media such as Plaintiff’s computer hard drive is classified at the highest level of classification of data contained therein. (*Id.* at ¶ 19.) Thus, because Plaintiff’s computer contains files with TOP SECRET SCI information, the hard drive is classified at the TOP SECRET SCI level. (*Id.*)

⁹ Plaintiff may assert that legislative privilege applies to her return of property claim, but it is well established that Congress itself controls legislative privilege, not individual Congressional employees. *See Gravel v. United States*, 408 U.S. 606, 621-22 n. 13 (1972) (noting that a Senator’s aide’s invocation of legislative privilege “can be repudiated and thus waived by the Senator”). In this case, HPSCI has decided not to assert any claim of legislative privilege over the property at issue. Similarly, Plaintiff’s contention that HPSCI’s mere review of the seized property somehow constitutes a violation of her rights is also unfounded. The NSA does not have the authority to agree to the release of information which originated from another federal entity absent the consent of the originator. (Miriam P. Decl. ¶ 9.) Furthermore, Plaintiff’s HPSCI NDA provides a clear basis for HPSCI to review the information at issue. (Dick Decl., Ex. 4 at ¶ 7 (agreeing to surrender protected information to HPSCI)).

The government is not able to simply delete the files containing classified information from the hard drive and return the hard drive to Plaintiff. That is because various complications can, and do, subvert the complete effectiveness of techniques designed to overwrite deleted files. (Charles E. Decl. ¶ 6.) For example, technical issues within hard drives, such as unreadable, or “bad”, sectors can prevent traditional forensic tools from accessing those areas. (*Id.*) The government is not aware of a technical solution that completely ensures the removal of data from a computer hard drive that does not result in the total destruction and inability to use the computer. (*Id.*)

Although the government cannot return Plaintiff’s computer without first erasing all of the data off of it, the government is willing and able to return any non-classified and non-protected common user files on identified areas of the computer to Plaintiff via portable storage media (such as a CD or DVD). Prior to returning any computer files, the government is prepared to conduct an automated search of the files using a key word list designed to identify classified or protected information. Any files that do not result in a “hit” on this key word list could be returned to Plaintiff without any further review, while any files that do return a “hit” would need to be reviewed by the NSA and/or HPSCI to determine whether the files contain classified or protected information. Any files which do not contain classified or protected information based on this manual review can also be returned to Plaintiff on portable storage media.¹⁰

¹⁰ The government also notes that it has no desire to preserve or maintain the property containing classified or protected information that it has not returned. (Dick Decl. ¶ 11; Miriam P. Decl. ¶ 20.) The government’s interest in such property is solely in ensuring the non-disclosure of sensitive information related to national security. (*Id.*) Thus, the government is willing to agree to destroy any property containing classified or protected information not returned to Plaintiff, to the extent that will address any concerns Plaintiff may have about the ultimate disposition of such property. (*Id.*)

V. CONCLUSION

For the foregoing reasons, Plaintiff is not entitled to return of the property retained by the government. Thus, Defendant respectfully requests that the Court grant Defendant's motion for summary judgment, deny Plaintiff's motion for return of property, and dismiss this action with prejudice.

DATED this 30th day of September 2014.

Respectfully submitted,

S. AMANDA MARSHALL
United States Attorney
District of Oregon

/s/ James E. Cox, Jr.
JAMES E. COX, JR.
Assistant United States Attorney
Attorneys for Defendant

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing **Defendant's Motion for Summary Judgment and Memorandum in Support** was placed in a postage prepaid envelope and deposited in the United States Mail at Portland, Oregon on September 30, 2014, addressed to:

Diane Roark
2000 N. Scenic View Dr.
Stayton, OR 97383

And was sent via email to the following email address:

gardenofeden@wvi.com

/s/ James E. Cox, Jr.
JAMES E. COX, JR.

NOV 1 1 2006 4 10 PM H

AUG. 29. 2006 10:35AM

NO. 557 P. 3

NO. 205 P. 1

SFN: _____

SENSITIVE COMPARTMENTED INFORMATION NONDISCLOSURE AGREEMENT

An Agreement Between DIANE ROARK, and the United States.
(Name Printed or Typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to information or material protected within Special Access Programs, hereinafter referred to in this Agreement as Sensitive Compartmented Information (SCI). I have been advised that SCI involves or derives from intelligence sources or methods and is classified or is in the process of a classification determination under the standards of Executive Order 12958 or other Executive Order or statute. I understand and accept that by being granted access to SCI, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of SCI, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information or material have been approved for access to it, and I understand these procedures. I understand that I may be required to sign subsequent agreements upon being granted access to different categories of SCI. I further understand that all my obligations under this Agreement continue to exist whether or not I am required to sign such subsequent agreements.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of SCI by me could cause irreparable injury to the United States or be used to advantage by a foreign nation. I hereby agree that I will never divulge anything marked as SCI or that I know to be SCI to anyone who is not authorized to receive it without prior written authorization from the United States Government department or agency (hereinafter Department or Agency) that last authorized my access to SCI. I understand that it is my responsibility to consult with appropriate management authorities in the Department or Agency that last authorized my access to SCI, whether or not I am still employed by or associated with that Department or Agency or a contractor thereof, in order to ensure that I know whether information or material within my knowledge or control that I have reason to believe might be SCI, or related to or derived from SCI, is considered by such Department or Agency to SCI. I further understand that I am also obligated by law and regulation not to disclose any classified information or material in an unauthorized fashion.

4. In consideration of being granted access to SCI and of being assigned or retained in a position of special confidence and trust requiring access to SCI, I hereby agree to submit for security review by the Department or Agency that last authorized my access to such information or material, any writing or other preparation in any form, including a work of fiction, that contains or purports to contain any SCI or description of activities that produce or relate to SCI or that I have reason to believe are derived from SCI, that I contemplate disclosing to any person not authorized to have access to SCI or that I have prepared for public disclosure. I understand and agree that my obligation to submit such preparations for review applies during the course of my access to SCI and thereafter, and I agree to make any required submissions prior to discussing the preparation with, or showing it to, anyone who is not authorized to have access to SCI. I further agree that I will not disclose the contents of such preparation to any person not authorized to have access to SCI until I have received written authorization from the Department or Agency that last authorized my access to SCI that such disclosure is permitted.

5. I understand that the purpose of the review described in Paragraph 4 is to give the United States a reasonable opportunity to determine whether the preparation submitted pursuant to Paragraph 4 sets forth any SCI. I further understand that the Department or Agency to which I have made a submission will act upon it, coordinating within the Intelligence Community when appropriate, and make a response to me within a reasonable time, not to exceed 30 working days from date of receipt.

6. I have been advised that any breach of this Agreement may result in the termination of my access to SCI and removal from a position of special confidence and trust requiring such access, as well as the termination of my employment or other relationships with any Department or Agency that provides me with access to SCI. In addition, I have been advised that any unauthorized disclosure of SCI by me may constitute violations of United States criminal laws, including the provisions of Sections 793, 794, 798 and 952, Title 18, United States Code, and of Section 783(b) Title 50, United States Code. Nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

7. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement. I have been advised that the action can be brought against me in any of the several appropriate United States District Courts where the United States Government may elect to file the action. Court costs and reasonable attorney's fees incurred by the United States Government may be assessed against me if I lose such action.

8. I understand that all information to which I may obtain access by signing this Agreement is now and will remain the property of the United States Government unless and until otherwise determined by an appropriate official or final ruling of a court of law. Subject to such determination, I do not now nor will I ever possess any right, interest, title, or claim whatsoever to such information. I agree that I shall return all materials that may have come into my possession or upon the conclusion of my employment or other relationship with the United States Government entity providing me access to such materials. If I do not return such materials upon request, I understand this may be a violation of Section 793, Title 18, United States Code.

9. Unless and until I am released in writing by an authorized representative of the Department or Agency that last provided me with access to SCI, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to SCI, and at all times thereafter.

10. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect. This Agreement concerns SCI and does not set forth such other conditions and obligations not related to SCI as may now or hereafter pertain to my employment by or assignment or relationship with the Department of Agency.

11. I have read this Agreement carefully and my questions, if any, have been answered to my satisfaction. I acknowledge that the briefing officer has made available Sections 793, 794, 798 and 952 of Title 18, United States Code, and Section 783(b) of Title 50, United States Code, and Executive Order 12958, as amended, so that I may read them at this time.

FORM 4414

NOV. 1. 2006 4: 28 PM H

NO. 557 P. 4

AUG. 29. 2006 10: 53 AM

NO. 206 P. 1

S. 2043886

ja

12. I hereby assign to the United States Government all rights, title and interest, and all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation not consistent with the terms of this Agreement.

13. These restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations rights or liabilities created by Executive Order 12958; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the Military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 USC 421 et seq.) (governing disclosures that could expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Section 641, 793, 794, 798 and 952 of Title 18, United States Code, and Section 4 (b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights sanctions and liabilities created by said Executive Order and listed statutes are incorporated into the Agreement and are controlling.

14. This Agreement shall be interpreted under and in conformance with the law of the United States.

15. I make this Agreement without any mental reservation or purpose of evasion.

Mimi Roark ✓ 24 July 01
Signature Date

The execution of this Agreement was witnessed by the undersigned who accepted it on behalf of the United States Government as a prior condition of access to Sensitive Compartmented Information.

WITNESS and ACCEPTANCE:

Charles 24 July 01
Signature Date

SECURITY BRIEFING / DEBRIEFING ACKNOWLEDGEMENT

[Redacted]

(SPECIAL ACCESS PROGRAMS BY INITIALS ONLY)

[Redacted] DIANE ROARK [Redacted]
SSN (See Notice Below) Printed or Typed Name Organization

BRIEF DATE 24 July 01

I hereby acknowledge that I was briefed on the above SCI Special Access Program(s):

Mimi Roark ✓
Signature of Individual Briefed

DEBRIEF DATE _____

Having been reminded of my continuing obligation to comply with the terms of this Agreement, I hereby acknowledge that I was debriefed on the above SCI Special Access Program(s):

Signature of Individual Debriefed

I certify that the briefing presented by me on the above date was in accordance with relevant SCI procedures.

Charles [Redacted] [Redacted]
Signature of Briefing Officer SSN (See Notice Below)

Charles [Redacted] [Redacted]
Printed or Typed Name Organization (Name and Address)

NOTICE: The Privacy Act, 5 U.S.C. 522a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above, 2) determine that you access to the information indicated has terminated, or 3) certify that you have witnessed a briefing or debriefing. Although disclosure of your SSN is not mandatory, your failure to do so may impede such certifications or determinations.

Not Reported in F.Supp.2d, 2012 WL 4069746 (D.Md.)
(Cite as: 2012 WL 4069746 (D.Md.))

H

Only the Westlaw citation is currently available.

United States District Court,
D. Maryland.
John WIEBE, et al., Plaintiff
v.
NATIONAL SECURITY AGENCY, et al., Defendant.

Civil Action No. RDB-11-3245.
Sept. 14, 2012.

John K. Wiebe, Westminster, MD, pro se.

William E. Binney, Severn, MD, pro se.

Diane S. Roark, Stayton, OR, pro se.

Edward F. Loomis, Baltimore, MD, pro se.

Thomas A. Drake, Glenwood, MD, pro se.

Thomas H. Barnard, Office of the U.S. Attorney,
Baltimore, MD, for Defendant.

REPORT AND RECOMMENDATION

STEPHANIE A. GALLAGHER, United States Magistrate Judge.

*1 This matter has been referred to me for report and recommendation. [ECF No. 8]. Five individual petitioners have filed motions under Fed. R.Crim. Proc. 41(g), seeking return of certain property seized by government agents. The five cases have been consolidated for disposition in this Court. [ECF Nos. 12, 16, 18]. The Complaint brought by one of those five Petitioners, Diane Roark, has been dismissed for improper venue. [ECF No. 59]. Respondents National Security Agency and Federal Bureau of Investigation (collectively, “the Government”) have filed a Motion to Dismiss or, in the alternative, for Summary Judgment. [ECF No. 46]. Two of the remaining four Petitioners, William E. Binney and John K.

Wiebe, have filed counter-Motions for Summary Judgment [ECF Nos. 49, 53]. I have reviewed the motions and the oppositions and replies thereto. I also held a hearing on the motions on August 23, 2012. For the reasons set forth below, I recommend that the Government’s Motion for Summary Judgment be granted in part and denied in part, and that Petitioners’ Motions for Summary Judgment be denied.

I. Background

During the course of a criminal investigation, on July 26, 2007, the Government searched the residences of Petitioners Wiebe and Binney pursuant to search warrants. On that same date, Government agents searched the residence of Petitioner Edward Loomis after obtaining Mr. Loomis’s consent. On November 28, 2007, Government agents searched the residence of Petitioner Thomas Drake pursuant to a search warrant. During each search, agents seized evidence including documents, computer accessories such as disks or CD Roms (“disks”), and computer hard drives (“HDDs”). Petitioners Wiebe, Binney, and Loomis were never charged with criminal conduct. The Government obtained an indictment against Petitioner Drake. *United States v. Drake*, RDB-10-0181 [ECF No. 1]. Eventually, Mr. Drake pled guilty to a misdemeanor offense of exceeding authorized use of a computer, and all remaining charges were dismissed. *Id.* [ECF No. 169]

Although some of the seized items have been returned to the Petitioners, the Government has refused to return other seized evidence.^{FN1} The information contained in the disputed items falls into one of four categories: classified information, information protected by the National Security Agency Act of 1959 (“NSAA information”), government information controlled by other government agencies (“OGA information”), and unprotected information.^{FN2} Through this action, Petitioners seek return of each disputed item in its entirety.

^{FN1}. The Government has not returned

Not Reported in F.Supp.2d, 2012 WL 4069746 (D.Md.)
 (Cite as: 2012 WL 4069746 (D.Md.))

two HDDs from Petitioner Wiebe, one HDD, three disks and 84 pages of paper documents from Petitioner Binney, one HDD from Petitioner Loomis, and seven HDDs, three disks, and 4526 pages of paper documents from Petitioner Drake. Collectively, those items will be called “the disputed items.” Other items have been returned to Petitioners, and Petitioners have abandoned their claims to certain items.

FN2. Unprotected information refers to any information that is non-classified, non-NSAA, or non-OGA information. For example, unprotected information includes Petitioners' personal data and family photographs.

The Government has used the following process to evaluate each disputed item. A Special Agent, Tony T., reviewed the data contained in each item. Tony T. identified potentially classified and protected information. Decl. of Tony T. ¶¶ 7–10. Tony T. then forwarded a subset of material he believed to be classified or protected to Steven T., an “original TOP SECRET classification authority.” Decl. of Steven T. ¶ 1. As an original TOP SECRET classification authority, Steven T. is responsible for confirming the classification of information. Decl. of Steven T. ¶ 7. Steven T. determined that each of the disputed items contains some classified information, NSAA information, or OGA information. Decl. of Steven T. ¶¶ 8–12. According to Steven T.'s Affidavit, that material is protected from release. Decl. of Steven T. ¶¶ 10 n. 5, 13–14.

II. Legal Standards

*2 Under [Federal Rule of Civil Procedure 8\(a\)\(2\)](#), a complaint must contain a “short and plain statement of the claim showing that the pleader is entitled to relief.” [Federal Rule of Civil Procedure 12\(b\)\(6\)](#) authorizes the dismissal of a complaint if it fails to state a claim upon which relief can be granted; therefore, “the purpose of [Rule 12\(b\)\(6\)](#) is to test the sufficiency of a complaint and not to re-

solve contests surrounding the facts, the merits of a claim, or the applicability of defenses.” [Presley v. City of Charlottesville](#), 464 F.3d 480, 483 (4th Cir.2006); see [McBurney v. Cuccinelli](#), 616 F.3d 393, 408 (4th Cir.2010) (Gregory, J., concurring) (citation omitted). A complaint must be dismissed if it does not allege “enough facts to state a claim to relief that is plausible on its face.” [Bell Atl. Corp. v. Twombly](#), 550 U.S. 544, 570, 127 S.Ct. 1955, 167 L.Ed.2d 929 (2007). “Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice” to plead a claim. [Ashcroft v. Iqbal](#), 556 U.S. 662, 678, 129 S.Ct. 1937, 173 L.Ed.2d 868 (2009). The plausibility standard requires that the pleader show more than a sheer possibility of success, although it does not impose a “probability requirement.” [Twombly](#), 550 U.S. at 556. When considering a motion to dismiss under [Rule 12\(b\)\(6\)](#), this Court accepts as true the facts alleged in Plaintiff's Complaint. See [Aziz v. Alcolac, Inc.](#), 658 F.3d 388, 390 (4th Cir.2011).

[Rule 56 of the Federal Rules of Civil Procedure](#) provides that a court “shall 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\(c\)](#). A material fact is one that “might affect the outcome of the suit under the governing law.” [Anderson v. Liberty Lobby, Inc.](#), 477 U.S. 242, 248, 106 S.Ct. 2505, 91 L.Ed.2d 202 (1986). A genuine issue over a material fact exists “if the evidence is such that a reasonable jury could return a verdict for the nonmoving party.” *Id.* In considering a motion for summary judgment, a judge's function is limited to determining whether sufficient evidence exists on a claimed factual dispute to warrant submission of the matter to a jury for resolution at trial. *Id.* at 249.

In undertaking this inquiry, this Court must consider the facts and all reasonable inferences in the light most favorable to the nonmoving party. [Ricci v. DeStefano](#), 557 U.S. 557, 129 S.Ct. 2658, 174 L.Ed.2d 490 (2009) (quoting [Scott v. Harris](#),

Not Reported in F.Supp.2d, 2012 WL 4069746 (D.Md.)
(Cite as: 2012 WL 4069746 (D.Md.))

550 U.S. 372, 380, 127 S.Ct. 1769, 167 L.Ed.2d 686 (2007)). However, this Court must also abide by its affirmative obligation to prevent factually unsupported claims and defenses from going to trial. *Drewitt v. Pratt*, 999 F.2d 774, 778–79 (4th Cir.1993). If the evidence presented by the non-moving party is merely colorable, or is not significantly probative, summary judgment must be granted. *Anderson*, 477 U.S. at 249–50. On the other hand, a party opposing summary judgment must “do more than simply show that there is some metaphysical doubt as to the material facts.” *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 586, 106 S.Ct. 1348, 89 L.Ed.2d 538 (1986); see *In re Apex Express Corp.*, 190 F.3d 624, 633 (4th Cir.1999). This Court has previously explained that a “party cannot create a genuine dispute of material fact through mere speculation or compilation of inferences.” *Shin v. Shalala*, 166 F.Supp.2d 373, 375 (D.Md.2001) (citations omitted).

*3 Fed. R.Crim. Proc. 41(g) governs motions for the return of property where an individual is “aggrieved by an unlawful search and seizure or by the deprivation of property.”^{FN3} A Rule 41(g) motion for return of property is typically granted if the related prosecution has ended, but should be denied if the government establishes a “continuing interest” in the property. See *United States v. Duncan*, 918 F.2d 647, 654 (6th Cir.1990).

FN3. Fed.R.Crim.P. 41(g) states:

Motion to Return Property. A person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return. The motion must be filed in the district where the property was seized. The court must receive evidence on any factual issue necessary to decide the motion. If it grants the motion, the court must return the property to the movant, but may impose reasonable conditions to protect access to the property and its use in later proceedings.

III. Arguments

A. Petitioners Have Standing To Sue.

Initially, the Government contends that Petitioners lack standing to pursue their claims because they have no possessory interest in government property. That argument is unavailing. Rule 41(g) petitioners have standing if they are able to show a “sufficient interest” in the seized items. *Matthews v. United States*, 917 F.Supp. 1090, 1104 (E.D.Va.1996). This is a “comparatively low” threshold, merely requiring the movants to allege ownership and to provide some evidence of ownership. *Id.*; see also *United States v. \$191,910 in U.S. Currency*, 16 F.3d 1051, 1057 (9th Cir.1994) (stating that although a party need not have an “ownership” interest in seized property to have standing, mere unexplained possession of property is insufficient).

Here, Petitioners have alleged ownership and have provided evidence of ownership of the disputed items. The disputed items are not, as the Government suggests, entirely government property. Although some government property may be contained within the disks, HDDs, and documents, many of the disputed items also contain Petitioners' professional and personal information. Petitioners' obvious ownership interest in their personal information is not eviscerated by the simultaneous presence of government information on the disputed items. Because Petitioners have established a sufficient ownership interest in information contained in the disputed items, and because they no longer have possession of those items, the Petitioners have established a sufficient deprivation of property to trigger Rule 41(g). As such, the complex issues presented should not be rejected via a threshold standing analysis.

B. The Government's Assertions of Classification and Statutory Protection Are Not Subject to Judicial Review.

The next issue is whether any classified, NSAA, or OGA information exists on the disputed

Not Reported in F.Supp.2d, 2012 WL 4069746 (D.Md.)
(Cite as: 2012 WL 4069746 (D.Md.))

items. The Government has asserted that each disputed item contains classified information, NSAA information that is protected under the National Security Agency Act of 1959, 50 U.S.C. § 402; 18 U.S.C. § 798; and Section 102A(i)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004, 30 § U.S.C. 403–1(i)(1), or OGA information. Decl. of Steven T. ¶¶ 8–10. Petitioners suggest that the Government's determinations are subject to judicial review. The Government contends that it alone determines whether information is classified, NSAA protected, or OGA. A review of governing law establishes that the Government's position is correct as to classified information and NSAA information. However, judicial review of the alleged OGA information is not precluded on the current record before the Court.

*4 Although Petitioners assert that the Government has an established record for improperly classifying or over-classifying information, the Government's classification determinations are not subject to challenge in court. See *United States v. Smith*, 750 F.2d 1215, 1217 (4th Cir.1984) (stating that the government may determine what is classified, and noting that neither the courts nor any defendant may challenge or question such a classification). In *United States v. Marchetti*, the Fourth Circuit held that a former Central Intelligence Agency (“CIA”) employee could not disclose classified information unless that information was already in the public domain. 466 F.2d 1309, 1317 (4th Cir.1972). Importantly, the court also held that if the CIA denied the employee the ability to publish certain material, the only classification issues that courts could review were whether the government had identified the information as classified, and if so, whether the information had previously entered the public domain. *Id.* at 1318. In other words, the court could not review the propriety of the government's classification of information. See *id.* The court reasoned that Article II § 2 confers broad powers upon the Executive in controlling relations with foreign states and conducting national defense, and that the CIA is an executive agency whose activities are

closely related to these functions. *Id.* at 1317. As such, the court held that the CIA's classification system is “part of the executive function beyond the scope of judicial review.” *Id.* at 1317; see also *United States v. Collins*, 720 F.2d 1195, 1198 n. 2 (11th Cir.1983) (noting that it is the Executive's responsibility to classify information, not the judiciary's).

The rationale precluding judicial review of classification decisions is equally applicable to NSAA information. The National Security Agency (“NSA”) is also an executive agency whose functions “closely relate” to conducting national defense. See Decl. of Steven T. ¶¶ 3–6. As such, designation of material as statutorily protected by the NSAA is as much a part of the executive function as classification. By analogy, then, judicial review of the Government's designation of material as NSAA information would be improper. *C.f. Marchetti*, 466 F.2d at 1317; *Smith*, 750 F.2d at 1217. In addition, this Court has previously held that the NSA holds a statutory privilege protecting against the disclosure of NSAA information relating to its activities. *United States v. Drake*, Criminal No. RDB 10–181, 2011 WL 2175007, at *5 (D.Md. June 2, 2011).^{FN4} Where the Government has identified information contained within the disputed items as classified or NSAA information, the law prevents this Court from assessing the propriety of those decisions.

FN4. The February 9, 2012 letter to Petitioner Wiebe and Counsel from Judge Richard D. Bennett [ECF No. 7], cited by Petitioners, simply noted that the parties dispute the classification of this information, and appointed this Court to address this matter. This statement did not indicate a position on the Court's jurisdiction to review the government's classification decisions.

The third category as to which the Government has asserted protection is OGA information. According to the Government, an OGA designation is

Not Reported in F.Supp.2d, 2012 WL 4069746 (D.Md.)
(Cite as: 2012 WL 4069746 (D.Md.))

placed on information that originated with another federal Agency or Department. *See* Decl. of Steven T. ¶ 10 n. 5. The Government has established that the OGA information at issue has not been released to the general public. Decl. of Steven T. ¶ 10 n. 5. However, the Government has not identified the federal Agency or Department in question, and has not even provided any general information about its duties. The record does not establish whether the information derived from the Department of Defense, the Department of Agriculture, or the General Services Administration. As such, the Government has neither established any connection between the OGA information and important interests of national security, nor has it provided any indication that the OGA information is classified by the other agency or protected by any statute. On the current record, then, any designation of material as OGA information is subject to judicial review and challenge in court.

C. The Government Has Established a Continuing Interest in Classified, NSAA, and OGA Information.

*5 Petitioners seek the return of all of the seized items, including the classified, NSAA, and OGA information. The Government's position is that it retains a continuing interest in such information and that the information therefore need not be returned. Further, the Government asserts that Petitioners are not entitled to lawful possession of classified information. The Government is correct.

Pursuant to [Rule 41\(g\)](#), courts must determine if the government's retention of seized property is "reasonable," and must balance the government's need to retain the property against the individual's right to use the property. *In re Grand Jury Subpoena Duces Tecum Issued to: Roe & Roe, Inc.*, 49 F.Supp.2d 451, 452–53 (D.Md.1999). Generally, seized property other than contraband "should be returned to the rightful owner after the criminal proceedings have terminated." *United States v. Duncan*, 918 F.2d 647, 654 (6th Cir.1990). This right of return, however, is subject to "any continu-

ing interest the government has in the property." *Id.* (emphasis added). What constitutes a government interest "may take different forms as long as it is a legitimate interest." *Id.*; *see Roe & Roe, Inc.*, 49 F.Supp.2d at 453 (noting that the Government must provide a "legitimate reason" to maintain possession of the property); *Sovereign News Co. v. United States*, 690 F.2d 569, 577 (6th Cir.1982) (use in investigation); *United States v. Francis*, 646 F.2d 251, 263 (6th Cir.1981) (right to levy); *United States v. Sabatino*, Nos. 07–2460–cr(L), 08–0628–cr(CON), 2009 WL 248009, at *1 (2d Cir. Feb. 3, 2009) (holding that the government had a continuing interest in photographs of petitioner's co-conspirators because their return to petitioner would pose a legitimate safety threat to others).

Here, the Government has established a sufficient continuing interest in the classified information. Classified information has been defined as "any information or material that has been determined by the United States Government pursuant to an Executive order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security." *Smith*, 750 F.2d at 1217 (citing the Classified Information Procedures Act, 18 U.S.C. app. 3); *see Exec. Order No. 13526*, Part 6, Sec. 6.1(i), 75 Fed.Reg. 707 (Dec. 29, 2009) ("classified information" is defined as "information that has been determined ... to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form."). Pursuant to 50 U.S.C. § 435(a), the President "shall establish procedures to govern access to classified information." Congress also required that the President's established procedures must, at a minimum, provide that no executive branch employee may receive access to classified information unless the government has performed a background investigation and has determined that such access is "clearly consistent" with its national security interests. 50 U.S.C. 435(a)(1).

*6 The President, pursuant to this authority, mandated that a person may only receive access to

Not Reported in F.Supp.2d, 2012 WL 4069746 (D.Md.)
(Cite as: 2012 WL 4069746 (D.Md.))

classified information if an agency has determined that the person is eligible, the person has signed a non-disclosure agreement, and the person needs to know the information. *Exec. Order No. 13526*, Part 1, Sec. 4.1(a), *75 Fed.Reg. 707 (Dec. 29, 2009)*. Here, it is undisputed that Petitioners do not hold security clearances, and that no agency has determined that Petitioners may have access to classified material. As such, the Government has established a continuing interest in maintaining the classified information and in not sharing the classified information with Petitioners. Moreover, the Petitioners may not lawfully obtain the classified information they seek.^{FN5}

^{FN5}. Each of the Petitioners' HDDs, other than Petitioner Drake's HDD, labeled Item 11, has been found to contain classified information. Decl. of Steven T. ¶ 9. The HDDs themselves are now considered classified because they contain classified information. Decl. of Steven T. ¶ 9. However, as addressed below, the unprotected information contained on those HDDs could be returned to Petitioners by copying the information onto an unclassified device.

The Government has also established a sufficient continuing interest in the unclassified NSAA information. The National Security Agency Act of 1959, Section 6(a), states that

“nothing in this Act or any other law ... shall be construed to require the disclosure of the organization or any function of the National Security Agency, or any information with respect to the activities thereof, or of the names, titles, salaries, or number of the persons employed by such an agency.”

In *Drake*, the Court held that the NSAA created a statutory privilege protecting the NSA against the disclosure of unclassified information “relating to” its activities. *Drake*, 2011 WL 2175007, at *5. Here, the Government has shown that some of the

information sought is protected by the NSAA. *See* Decl. of Steven T., ¶¶ 8, 10, 11, 12. Accordingly, the Government has established a continuing interest in the NSAA information, and the Court cannot require the Government to disclose the NSAA information sought by the Petitioners.^{FN6} *See* National Security Agency Act of 1959, Section 6(a); *Drake*, 2011 WL 2175007, at *5.

^{FN6}. Petitioner Drake's HDD, labeled Item 11, is now considered protected under the NSAA because it contains NSAA information. Decl. of Steven T. ¶¶ 8–9.

Last, although the Government's OGA designation is not dispositive, Petitioners are not entitled to the return of OGA information. As noted above, a Petitioner's right to receive its property after a criminal investigation is terminated is subject to “any continuing interest the government has in the property.” *Duncan*, 918 F.2d at 654 (emphasis added). The Government asserts a sufficient and legitimate interest in OGA information as government property that has not been released to the public. Mot. at 20. Information generated by the government is “clearly [the government's] property.” *United States v. Berlin*, 707 F.Supp. 832, 839 (E.D.Va.1987). Because the alleged OGA information “clearly originated from another federal Agency or Department,” Decl. of Steven T. ¶ 10 n. 5, the Government has proven that the alleged OGA information is government information, meaning that it is also government property. *See Berlin*, 707 F.Supp. at 839. In addition, the Government has not released the alleged OGA information to the general public, Decl. of Steven T. ¶ 10 n. 5, adding to the Government's interest in maintaining sole possession of this information. Certainly, the Government's interest might even be stronger if it demonstrates that this material has not been released because it is important to national security. However, as noted above, the Government must merely prove that it has “any” legitimate interest in the property to maintain possession. *Duncan*, 918 F.2d at 654. The Government's interest in its own property that has not been

Not Reported in F.Supp.2d, 2012 WL 4069746 (D.Md.)
(Cite as: 2012 WL 4069746 (D.Md.))

released to the public is sufficient for purposes of Rule 41(g). As such, if the Government establishes that its alleged designation of OGA information is proper, Petitioners should not be entitled to its return.

D. Summary Judgment is Inappropriate as to the Unprotected Information.

*7 Petitioners have sought the return of each disputed item in its entirety, including the unprotected information contained therein. The Government's theory is that the classified, NSAA, and OGA information constitutes "contraband," and that the HDDs, disks, and documents containing the classified material constitute "derivative contraband." The Government takes the position that it does not have to return "derivative contraband" to the Petitioners. However, a genuine issue of material fact exists as to whether any of the disputed information is "contraband" or "derivative contraband." As a result, all parties' motions for summary judgment should be denied.

Contraband is defined as an "object the possession of which, without more, constitutes a crime." *United States v. Mettetal*, No. Civ.A. 396CR30034-00, 2006 WL 1195777, at *2 (W.D.Va. May 3, 2006) (quoting *One 1958 Plymouth Sedan v. Pennsylvania*, 380 U.S. 693, 699, 85 S.Ct. 1246, 14 L.Ed.2d 170 (1965)). Derivative contraband is property that may be possessed lawfully, but is used in an unlawful manner or for an unlawful purpose. See *One 1958 Plymouth Sedan*, 380 U.S. at 699; *United States v. Felici*, 208 F.3d 667, 670 (8th Cir.2000).

Citing only *United States v. Moussaoui*, No. CR. 01-455- A, 2002 WL 32001771, at *4 (E.D.Va. Sept.26, 2002), the Government argues that "[c]lassified material in the possession of someone not cleared to have it is considered 'contraband.'" Mot. at 15. That citation provides no precedential support for the assertion, because it refers not to a determination made by a court, but to a letter written by counsel for the Government in the *Moussaoui* case. See *id.* The mere fact that the

Government's letter was unsealed by the court and attached to the order does not indicate in any way that the *Moussaoui* judge adopted its assertions. See *id.*

In fact, no court has determined that classified material in the possession of someone not cleared to have it is contraband *per se*. To prove that Petitioners possessed contraband or derivative contraband, therefore, the Government must prove that the Petitioners obtained or used the information unlawfully. ^{FN7} See *One 1958 Plymouth Sedan*, 380 U.S. at 699; *Felici*, 208 F.3d at 670 (stating that derivative contraband is "property that may be lawfully possessed but which became forfeitable because of unlawful use."). The Government has not shown that the information was classified or otherwise protected when Petitioners initially obtained it, ^{FN8} or that Petitioners took or used any information unlawfully or in violation of their Contractor Security Agreements.

^{FN7}. If, for example, the Government proves that Petitioners stole the classified or NSAA information, or somehow used this information unlawfully, the Government may be able to prove that this information constitutes derivative contraband.

^{FN8}. The Government conceded at the hearing that it is unaware whether the disputed information was classified or protected when Petitioners obtained the information.

In fact, Petitioners contend that their actions were fully lawful. Petitioner Drake asserts that he "lawfully retained unclassified protected communications information at his residence when he served as a material witness for two 9/11 Congressional investigations" and that he "was a whistleblower under the Intelligence Community Whistleblower Protection Act of 1978 when in contact with Congress and the DoD." Drake Opp'n at 1-2. Petitioner Loomis seemingly posits ^{FN9} that he and Petitioner Binney received permission from an in-

Not Reported in F.Supp.2d, 2012 WL 4069746 (D.Md.)
(Cite as: 2012 WL 4069746 (D.Md.))

tellectual property attorney in the Office of the General Counsel to take some of the disputed information and to use it to form a private business. *See Loomis Opp'n* at 3, 10. As such, a genuine issue of material fact is present. The Government has not established that Petitioners acted unlawfully in obtaining or using any disputed information. Without such proof of unclean hands, the disputed information cannot be labeled as “contraband” or “derivative contraband.”

FN9. Courts liberally construe pleadings and briefs from *pro se* litigants “to raise the strongest arguments they suggest.” *Burgos v. Hopkins*, 14 F.3d 787, 790 (2d Cir.2000). Therefore, although Petitioners did not place these facts in an affidavit, this Court will liberally construe *pro se* Petitioners' submissions as though they used the proper format.

*8 The Government next argues that it is not obligated to return any unprotected information, claiming that if an HDD is classified or NSAA protected, there is no legal requirement forcing the Government to copy unprotected files onto another media for return to Petitioners. *See Mot.* at 18. As noted above, however, seized property other than contraband “should be returned to the rightful owner after the criminal proceedings have terminated.” *Duncan*, 918 F.2d at 654; *see Marshall v. Duncan*, No. CA3-84-0503-F, 1984 WL 777, at *2 (N.D.Tex. June 19, 1984) (requiring the IRS to return duplicates of original documents requested by plaintiffs). Here, Petitioners seek return of personal information located on their seized HDDs. The Government has asserted no continuing interest in this unprotected information. Instead, at oral argument, the Government relies on the “undue burden” it would suffer to sift through and return the information. The law contains no “inconvenience exception” to the proposition that seized property should be returned to its lawful owner in the absence of a continuing Government interest. As such, there is no legal basis to grant summary judgment

in the Government's favor.

E. Petitioners' Other Arguments for Return of Classified Materials Are Unavailing.

1. The Government Did Not Have to Satisfy the Requirements of CAFRA.

Petitioners also seek return of the property pursuant to the Civil Asset Forfeiture Reform Act of 2000 (“CAFRA”), 18 U.S.C. § 983, arguing that the Government cannot retain the property because it failed to abide by CAFRA's guidelines. The Government counters that it has not sought and is not seeking forfeiture of the property, and therefore that CAFRA does not apply. The Government's position is correct.

CAFRA requires written notice to interested parties in nonjudicial civil forfeiture proceedings. 18 U.S.C. § 983(a)(1) (A). That notice must be sent within 60 days after the date of the seizure, and if the Government fails to send this notice, the Government must return the property. *Id.*; 18 U.S.C. § 983(a) (1)(F). Petitioners contend that because they received no such notice, the Government cannot retain the seized items.

This argument is flawed, first, because CAFRA does not require the Government to return “property that the person from whom the property was seized may not legally possess.” § 983(a)(1)(f). As explained above, Petitioners are not entitled to lawful possession of classified information. *See supra* Part III.C. The Government therefore cannot be forced to return information, which the Government has now established to be classified, pursuant to CAFRA.

Moreover, regarding all of the seized property, the Government is not seeking and has never sought forfeiture. Instead, the Government seized and held the property as evidence in a criminal investigation. When the Government seizes property for non-forfeiture purposes, the notice requirements of § 983(a)(1)(A) do not apply. *See Langbord v. United*

Not Reported in F.Supp.2d, 2012 WL 4069746 (D.Md.)
(Cite as: 2012 WL 4069746 (D.Md.))

States Dept. of Treasury, 645 F.Supp.2d 381, 388 (E.D.Pa.2009); *Celata v. United States*, No. 07-36088, 2009 WL 1385965 (9th Cir. May 19, 2009); *Chaim v. United States*, 692 F.Supp.2d 461, 465-66 (D.N.J.2010); Stefan Cassella, *The Civil Asset Forfeiture Reform Act of 2000: Expanded Government Forfeiture Authority and Strict Deadlines Imposed on All Parties*, 27 J. LEGIS. 97, 129 (2001). In fact, where the government is not pursuing forfeiture, "the only procedurally proper way to seek return of the property seized ... would be to file a motion pursuant to Fed.R.Crim.P. 41(g)." *Celata*, 2009 WL 1385965, at *1. Therefore, because the Government has not sought forfeiture, Petitioners are not entitled to the return of the disputed property under CAFRA.

2. The Legality of the Searches Resulting In the Property's Seizure Is Not Relevant.

*9 Petitioners' homes were searched either by consent, in the case of Mr. Loomis, or by search warrant, in the case of the other Petitioners. Petitioners wish to contest the validity of the warrants, the legality of the searches and seizures, and the voluntariness of the consent. A determination that the warrants, searches, and consent were unlawful, however, would not affect the outcome of the analysis under Rule 41(g). Therefore, this Court need not consider the Fourth Amendment issues.

First, even if Petitioners establish a Fourth Amendment violation, Petitioners still would not be entitled to the return of the classified, NSAA, and OGA information because the Government has a continuing interest in retaining this property. Rule 41(g), as a threshold matter, provides a remedy to petitioners who have been aggrieved by an unlawful search and seizure *or* by a deprivation of property. Because the Petitioners have already established a deprivation of property, *see supra* Part III.A., establishing an unlawful search or seizure is unnecessary. The only remaining inquiry under 41(g) is whether the government has a continuing interest in the disputed items. *See Duncan*, 918 F.2d at 654. As addressed above, the Government has a

continuing interest in the classified, NSAA, and OGA information, and establishing a Fourth Amendment violation would not diminish or vitiate this interest.

Moreover, proving that the Government violated the Fourth Amendment would not alter the appropriate analysis regarding the unprotected information. Issues of fact still remain as to whether the Petitioners lawfully or unlawfully obtained the classified, NSAA, and OGA information. *See supra* Part III.D. If the Government were to establish that Petitioners acted unlawfully, the classified or otherwise protected information might be considered contraband, and the unprotected information might be considered derivative contraband. *Id.* The Government is not required to return contraband or derivative contraband even if the initial searches or seizures violated the Fourth Amendment. *See United States v. One (1) 1971 Harley-Davidson Motorcycle Serial No. 4A25791H1*, 508 F.2d 351, 352 (9th Cir.1974); *United States v. Eighty-Eight Thousand, Five Hundred Dollars*, 671 F.2d 293, 297 (8th Cir.1982) (holding that both contraband and derivative contraband are forfeited even if there is an illegal search). If Petitioners acted lawfully, the information seized is not contraband, and the unprotected information is not derivative contraband. *See supra* Part III.D. As such, the Government would be required to return the unprotected information even if the searches and seizures were entirely lawful. In either scenario, then, establishing that the Government violated the Fourth Amendment would have no bearing on whether Petitioners may obtain return of information.

IV. CONCLUSION

For the reasons set forth above, I recommend that summary judgment in favor of the Government be granted in part and denied in part. The Government has established as a matter of law that the information it deems to be classified or NSAA information, including all eleven HDDs in question, cannot be returned to Petitioners. I recommend that the Government's motion for summary judgment be

Not Reported in F.Supp.2d, 2012 WL 4069746 (D.Md.)
(Cite as: 2012 WL 4069746 (D.Md.))

granted in part as to that issue. However, material facts remain in dispute regarding (1) whether or not the information labeled as “OGA information” is in fact OGA information, and (2) whether the unprotected information contained in the disputed items must be returned in an unclassified format. Because genuine issues of material fact exist on the current record, I recommend that summary judgment be denied to all movants relating to the OGA information and the unprotected information.

***10** If this report and recommendation is adopted, and the Government's motion for summary judgment is granted in part, there will be no further litigation regarding return of property the Government labels as classified or NSAA information. That material will not be returned to Petitioners. The Government may choose to provide additional evidence to permit the Court to evaluate its assertions as to the OGA information.

As to the unprotected information, at the hearing on this matter, the Government reiterated its willingness to return such content to the Petitioners. If the Government adheres to that position and wishes to agree to return the unprotected information in full, there will be no reason for fact discovery or for further motions. The Government will be providing the Petitioners voluntarily with the maximum recovery Petitioners could hope to achieve by litigating the case. In that circumstance, I recommend that I hold individual conference calls with the Government and each Petitioner to set firm and appropriate deadlines for the return of the unprotected information. During those calls, I will explore with each Petitioner whether the Petitioner can provide assistance to the Government to expedite its review and return of the material.

If the Government prefers to litigate whether or not the HDDs, disks, and documents constitute derivative contraband, and whether or not any of the material has to be returned, then I recommend that I confer with the parties to set a schedule for limited discovery and for an evidentiary hearing. The hearing, and the pre-hearing discovery, would be lim-

ited to (1) facts necessary to determine whether or not Petitioners engaged in any unlawful conduct or had “unclean hands;” and (2) facts necessary to determine the relationship between any unlawful conduct/unclean hands and Petitioners' use of the disputed items. Following that evidentiary hearing, I would prepare another report and recommendation outlining findings of fact regarding whether or not Petitioners engaged in any wrongdoing, and recommending whether or not the unprotected material has to be returned to Petitioners.

For the reasons stated herein, I recommend that Petitioners' Motions for Summary Judgment, [ECF Nos. 49, 53], be DENIED, and I further recommend that the Government's Motion for Summary Judgment, [ECF No. 46], be GRANTED in part and DENIED in part. I direct the Clerk to mail a copy of this Report and Recommendation to Petitioners at the addresses listed on the docket. Any objections to this Report and Recommendation must be served and filed within fourteen (14) days, pursuant to [Fed.R.Civ.P. 72\(b\)](#) and Local Rule 301.5.b.

D.Md.,2012.

Wiebe v. National Sec. Agency

Not Reported in F.Supp.2d, 2012 WL 4069746
(D.Md.)

END OF DOCUMENT

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

JOHN WIEBE, et al. *

Plaintiffs, *

Civil Action No.: RDB-11-3245

v. *

NATIONAL SECURITY AGENCY, et al. *

Defendants. *

* * * * *

MEMORANDUM OPINION AND ORDER

This matter is before the Court in these consolidated cases for consideration of Magistrate Judge Stephanie A. Gallagher’s Report and Recommendation (ECF No. 67) of September 14, 2012. On February 9, 2012, this Court referred these consolidated cases to Magistrate Judge Gallagher to conduct hearings, including evidentiary hearings if necessary, and to submit proposed findings of fact and recommendations for the disposition of this matter. *See* Order of Reference, ECF No. 8. In particular, Magistrate Judge Gallagher has submitted a Report and Recommendation regarding Respondent the Government’s Motion to Dismiss or, in the alternative, Motion for Summary Judgment (ECF No. 46), Petitioner William E. Binney’s Motion for Summary Judgment (ECF No. 49), and Petitioner John K. Wiebe’s Motion for Summary Judgment (ECF No. 53). These matters were fully briefed, and Magistrate Judge Gallagher held a hearing on these motions on August 23, 2012.

AUTHORITY FOR AND SCOPE OF REVIEW

Under 28 U.S.C. § 636(b)(1), Rule 72(a) of the Federal Rules of Civil Procedure, and Local Rule 305.1.b, an aggrieved party may file objections to or seek reconsideration of a

magistrate judge's ruling or report and recommendation within 14 days of its issuance. After considering these objections, the district court may modify or set aside any portion of the magistrate judge's order or recommendation if it is "clearly erroneous or is contrary to law." *See, e.g., Orpiano v. Johnson*, 687 F.2d 44, 47 (4th Cir. 1982).

RESULT OF REVIEW

The Court will not restate the status of the underlying cases and the nature of the dispute, relying instead on the statement of facts and procedural posture set forth in the Report and Recommendation of the Magistrate Judge.

The Court has carefully reviewed Magistrate Judge Stephanie A. Gallagher's Report and Recommendation (ECF No. 67), the objections of the consolidated Petitioners (ECF No. 73) and the Government (ECF No. 75), along with its legal arguments and the responsive arguments of the Petitioners and Respondents (ECF Nos. 76, 77). The Court approves the orders and recommendations by Magistrate Judge Gallagher and concludes that her determinations are neither clearly erroneous nor contrary to law. Moreover, after careful review of the objections by the Petitioners and Respondents, as well as the pertinent portions of the Report and Recommendation to which objection was made, this Court determines that those objections are unavailing. This Court fully agrees with the Magistrate Judge's conclusions.

For these reasons, the Court adopts the recommendation by Magistrate Judge Gallagher to GRANT IN PART and DENY IN PART the Government's Motion for Summary Judgment (ECF No. 46) and to DENY the Petitioners' Motions for Summary Judgment (ECF Nos. 49, 53).

CONCLUSION

For the foregoing reasons, the Court ADOPTS the reasoning of and AFFIRMS Magistrate Judge Stephanie A. Gallagher's Report and Recommendation (ECF No. 67), and rejects the objections submitted by the consolidated Petitioners (ECF No. 73) and the Government (ECF No. 75). Accordingly, it is ORDERED that:

1. The Report and Recommendation (ECF No. 67) of Magistrate Judge Stephanie A. Gallagher is ADOPTED AND APPROVED;
2. The Consolidated Petitioners' Objections (ECF No. 73) are OVERRULED;
3. The Respondents Federal Bureau of Investigation and National Security Agency's Objections (ECF No. 75) are OVERRULED;
4. Petitioner William E. Binney's Motion for Summary Judgment (ECF No. 49) is DENIED;
5. Petitioner John K. Wiebe's Motion for Summary Judgment (ECF No. 53) is DENIED;
6. The Respondent the Federal Bureau of Investigation and National Security Agency's Motion for Summary Judgment (ECF No. 46) is GRANTED IN PART and DENIED IN PART;
7. Pursuant to Federal Rule of Civil Procedure 56(a), JUDGMENT IS ENTERED in favor of the Government as to the information that it deems to be classified or NSAA information, including all eleven computer hard drives in question.

Date: March 27, 2013

_____/s/_____
Richard D. Bennett
United States District Judge

S. AMANDA MARSHALL, OSB # 953473

United States Attorney

District of Oregon

JAMES E. COX, JR., OSB # 085653

jim.cox@usdoj.gov

Assistant United States Attorney

United States Attorney's Office

District of Oregon

1000 SW Third Ave., Suite 600

Portland, Oregon 97204-2902

Telephone: (503) 727-1026

Facsimile: (503) 727-1117

Attorneys for Defendant United States

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

DIANE ROARK,

Case No.: 6:12-CV-01354-MC

Plaintiff,

v.

**DECLARATION OF MIRIAM P.¹ IN
SUPPORT OF DEFENDANT'S MOTION
FOR SUMMARY JUDGMENT**

UNITED STATES OF AMERICA,

Defendant.

¹ Section 6 of the National Security Agency Act of 1959, 50 U.S.C. § 3605 (Pub. L. No. 86-36) authorizes the National Security Agency (NSA) to protect from public disclosure, among other categories of information, the names of its employees. The undersigned declarant and the NSA employee referred to in the body of this declaration occupy non-public positions with the NSA. Thus, the names of these NSA employees are referred to by first name, last initial. The Agency is prepared to provide the full name of any employee in an *ex parte*, under seal filing should the Court so require.

I, Miriam P., hereby make the following declaration under penalty of perjury pursuant to 28 U.S.C. § 1746.

1. I am the Deputy Chief of Staff for Policy and Corporate Issues for the Signals Intelligence Directorate (SID) of the National Security Agency (NSA), an intelligence agency within the Department of Defense. I am responsible for, among other things, protecting NSA Signals Intelligence (SIGINT) activities, sources, and methods against unauthorized disclosures. Under Executive Order (E.O.) 12333, NSA is responsible for the collection, processing, analysis, production and dissemination of SIGINT information for the foreign intelligence and counterintelligence purposes of the United States. 46 Fed. Reg. 59941 (Dec. 4, 1981) as amended by Executive Order 13284 (2003), Executive Order 13355 (2004), 69 Fed. Reg. 53593 (Aug. 27, 2004); and Executive Order 13470 (2008).

2. I have been designated an original TOP SECRET classification authority under E.O. 13526, 75 Fed. Reg. 707 (Jan. 5, 2010), and Department of Defense Manual 5200.01, Information and Security Program, Vol. I (Feb. 24, 2012).

3. My statements herein are based upon my personal knowledge of NSA and SIGINT operations, my review of certain information, and the information available to me in my capacity as the Deputy Chief of Staff for Policy and Corporate Issues for the Signals Intelligence Directorate of NSA.

4. The NSA was established by Presidential Directive in 1952 as a separately organized agency within the Department of Defense under the direction, authority, and control of the Secretary of Defense. NSA's foreign intelligence mission includes the responsibility to collect, process, analyze, produce, and disseminate SIGINT information for foreign intelligence and

counterintelligence purposes, to support national and departmental missions, to include the conduct of military operations. See E.O. 12333, section 1.7 (c), as amended.

5. In performing its SIGINT mission, NSA exploits foreign signals to obtain intelligence information necessary to the national defense, national security, or the conduct of foreign affairs. NSA has developed a sophisticated worldwide SIGINT collection network that acquires, among other things, foreign and international electronic communications. The technological infrastructure that supports the NSA's foreign intelligence information collection network has taken years to develop at a cost of billions of dollars and untold human effort. It relies on sophisticated collection and processing technology.

6. In order to allow NSA to successfully perform its SIGINT mission, some of its activities must be kept secret. Original classification is the initial determination that NSA information requires, in the interest of national security, protection against unauthorized disclosure. There are three levels of classification that are based on the damage to national security that could be expected if the information were subject to unauthorized disclosure.

- a. "TOP SECRET" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security;
- b. "SECRET" shall be applied to information, the authorized disclosure of which reasonably could be expected to cause serious damage to the national security; and
- c. "CONFIDENTIAL" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

7. In addition to classification, NSA information may also be Sensitive Compartmented Information (SCI), which is "information that not only is classified for national security reasons

as Top Secret, Secret, or Confidential, but also is subject to special access and handling requirements because it involves or derives from particularly sensitive intelligence sources and methods.” 28 C.F.R. § 17.18(a). Because of the exceptional sensitivity and vulnerability of such information, these safeguards and access requirements exceed the access standards that are normally required for information of the same classification level. Specifically, this declaration references special intelligence (SI), a marking used to protect certain Communications Intelligence (COMINT), which is a subcategory of SCI. SI identifies SCI that was derived from exploiting cryptographic systems or other protected sources by applying methods or techniques, or from intercepted foreign communications.

8. As a TOP SECRET original classification authority pursuant to section 1.3 of E.O. 13526, it is one of my responsibilities to confirm the classification of NSA SIGINT information and/or information impacting NSA equities.

9. The NSA does not have the authority to agree to the release of classified or protected information that originates from another federal agency or department. When the question of disclosure of such information arises, the NSA refers the information and the issue of disclosure to the originating agency for a decision.

10. Through the exercise of my official duties, I have become familiar with the current litigation arising out of a request by plaintiff Diane Roark for the return of a computer and other items that I have been informed were seized by the Federal Bureau of Investigation (FBI). This declaration is provided in support of the government’s continuing interest in classified and/or protected information found in certain items that were seized at Plaintiff’s residence and therefore should not be returned to her.

11. It is my understanding that the FBI seized various documents/papers and a CD from plaintiff Roark's residence. I have conducted a classification review of a sampling of information in these items, using relevant authorities, such as classification guides and databases as applicable to determine the appropriate classification level of information contained in the paper documents/files.

12. Based on my authority as a TOP SECRET classification authority, I have determined that at least four of the paper documents in the possession of the FBI from the Roark search and seizure all contain information that is currently and properly classified information as reflected in the chart below, in accordance with E.O. 13526, and protected from release by statute, specifically Section 6 of the National Security Agency Act of 1959.

Log Item #	Description (type of item, # of pages, general nature of content)	Classification level of document
HC4	Commander Naval Security Group Slides, 18 pages	SECRET
HC11	Pre-publication Submission by Diane Roark, (first copy), 4 pages	SECRET//SI
HC12	Pre-publication Submission by Diane Roark, (second copy) 4 pages	SECRET//SI
HC13	Pre-publication Submission by Diane Roark, (third copy), 4 pages	SECRET//SI

13. Executive Order 13526, Section 1.4 provides that information may not be considered for classification unless its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security and pertains to one or more of eight specifically enumerated categories of information. The category of classified information to which the four documents listed above pertain is Section 1.4(c), intelligence activities (including covert action), intelligence sources and methods, or cryptology. Disclosure of the classified

information in these documents reasonably could be expected to cause serious damage to United States national security by compromising SIGINT intelligence sources, methods and/or activities. Specifically, item #HC4 contains Electronic Intelligence (ELINT) information that is currently and properly classified. ELINT, a subset of SIGINT, is technical and intelligence information derived from foreign non-communications electronic signals, such as radars and radar-jamming signals. Items #HC11, HC12 and HC13 contain COMINT information that is currently and properly classified. COMINT is technical and intelligence information derived from foreign communications signals and data. To provide additional information regarding these classified documents would lead to the disclosure of classified information.

14. Congress has specifically recognized the inherent sensitivity of the activities of the NSA. One of these statutes is a statutory privilege unique to NSA. NSA's statutory privilege is set forth in section 6 of the National Security Agency Act of 1959, 50 U.S.C. § 3605 (Public Law 86-36). Section 6 of the NSA Act provides that "[n]othing in this Act or any other law . . . shall be construed to require the disclosure of the organization or any function of the National Security Agency, of any information with respect to the activities thereof" By this language Congress expressed its finding that disclosure of any information relating to NSA activities is potentially harmful. In addition to being currently and properly classified in accordance with E.O. 13526, each of the four aforementioned documents is also exempt from public disclosure under Public Law 86-36. Information, however, need not be classified to be exempt from public disclosure in accordance with Public Law 86-36.

15. Based on my review of the information withheld from return to Plaintiff Roark, I have also determined that the following 19 items all contain information that is protected from release under Public Law 86-36:²

Log Item #	Description (# pages, type of item, general nature of content)
HC1	Email strings "Re: suggestions tonight?", 9 pages
HC2	Congressional Staff Visit, dated 24 June 1999, 2 pages
HC3	Memorandum for Commander, Naval Security Group Command, 2 pages
HC5	Set of miscellaneous documents, primarily faxes, 38 pages
HC7	Working Group April 19, 2001 CD
HC14	Initial Comments Regarding Specific Redactions 9/11/06, 5 pages
HC23	Notebook, At a Glance 2000, 90 pages
HC24	Notebook, 6/96 – Message log (audio), 55 pages
HC25	Notebook, tel. msg. 7/98 – 2/23/99, 71 pages
HC26	Notebook, Telephone msg 2/24/99 to 7/21/99, 68 pages
HC27	Notebook, msg 9/28/99 to 4/6/00, 63 pages
HC28	Notebook, msg 4/6/00 to 12/1/00, 69 pages
HC29	Notebook, 12/4/00 – , 67 pages
HC31	Notebook, Telecons 10/97-6/98, 69 pages
HC32	Notebook, Pocket Planner (Inside: 1990 calendar), 103 pages
HC33	Notebook, Week At a Glance (Inside: Appointments 1999), 101 pages
HC34	Notebook, (Back cover) 1995-96 Msg log (audio), 38 pages
HC35	Notebook, Press List Telecons 4/23/97 to 9/25/97, 42 pages
HC36	Notebook, msg 7/22-9/27/99, 51 pages

16. The foregoing documents are protected from disclosure by Public Law 86-36, Section 6, because they each reference the name(s) of NSA employees in non-public positions with the Agency.

² Due to the length of some of these documents and the difficulty in reading some of the handwritten notes, I have only confirmed the presence of NSA protected information in at least one location of each item. Thus, it is possible these items may also contain information classified in accordance with E.O. 13526.

17. I also reviewed four files that were on a computer hard disk drive (“HDD”) that the FBI seized from plaintiff Roark. Based on my authority as a TOP SECRET classification authority, I have determined that the files contain information that is currently and properly classified at the TOP SECRET//SI level in accordance with E.O. 13526. The information is also protected from release by statute, specifically Section 6 of the National Security Agency Act of 1959.

File and Description (file name, type of file, general nature of content)	Classification of Document or status as NSA protected information
WRC1864.tmp (temporary file), THIN THREAD, May 2002	TOP SECRET//SI
WRL0401.tmp (temporary file), THIN THREAD, May 2002	TOP SECRET//SI
WRL0718.tmp (temporary file), May 2002, THIN THREAD	TOP SECRET//SI
TT Description 3a.doc	TOP SECRET//SI

18. The category of classified information to which the information in these four files pertains is Section 1.4(c), intelligence activities (including covert action), intelligence sources and methods, or cryptology. Disclosure of the classified information reasonably could be expected to cause exceptionally grave damage to United States national security by compromising SIGINT intelligence sources, methods and/or activities. All four files contain COMINT information that is currently and properly classified. To provide additional information regarding the document would lead to the disclosure of classified information.

19. The HDD containing these files is an Information Storage Media (ISM) (i.e., a data storage object capable of being read from, or written to, by an Information System) and must be protected at the classification level of the information stored on the ISM. (NSA Policy 6-22, issued 3 January 2008 and revised 8 November 2013, "Labeling, Declassification, and Release of NSA/CSS Information Storage Media.") Therefore, plaintiff Roark's HDD currently and properly is classified TOP SECRET//SI.

20. NSA's assertion of interests in the foregoing material is for the purpose of ensuring that there is no disclosure of classified information and/or information exempt from public disclosure under Public Law 86-36. NSA has no interest in preserving any of the foregoing materials seized from plaintiff Roark. NSA is willing to destroy all copies of the foregoing materials in its possession.

21. Should the Court require additional details, I can provide a supplemental classified declaration *ex parte in camera* for the court's consideration.

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

Executed this 29th day of September 2014 at Fort Meade, Maryland.



MIRIAM P.

CERTIFICATE OF SERVICE

I hereby certify that on September 30, 2014 a copy of the foregoing **Declaration of Miriam P. in Support of Defendant's Motion for Summary Judgment** was placed in a postage prepaid envelope and deposited in the United States Mail at Portland, Oregon, , addressed to:

Diane Roark
2000 N. Scenic View Dr.
Stayton, OR 97383

And was sent via email to the following email address:

gardenofeden@wvi.com

/s/ James E. Cox, Jr.
JAMES E. COX, JR.

S. AMANDA MARSHALL, OSB # 953473

United States Attorney

District of Oregon

JAMES E. COX, JR., OSB # 085653

jim.cox@usdoj.gov

Assistant United States Attorney

United States Attorney's Office

District of Oregon

1000 SW Third Ave., Suite 600

Portland, Oregon 97204-2902

Telephone: (503) 727-1026

Facsimile: (503) 727-1117

Attorneys for Defendant United States

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

DIANE ROARK,

Case No.: 6:12-CV-01354-MC

Plaintiff,

v.

**DECLARATION OF DARREN M. DICK IN
SUPPORT OF DEFENDANT'S MOTION
FOR SUMMARY JUDGMENT**

UNITED STATES OF AMERICA,

Defendant.

I, Darren M. Dick, hereby make the following declaration under penalty of perjury pursuant to 28 U.S.C. § 1746. I make this declaration on personal knowledge and, if called upon to do so, I could and would competently testify to the following matters.

1. I serve as the Staff Director of the House Permanent Select Committee on Intelligence (“HPSCI”). I have served in that position since August 2013. Between January 2011 and August 2013, I served as the Deputy Staff Director.

2. This declaration relates to the review I conducted of certain documents that I understand were seized from plaintiff Diane Roark’s residence by the Federal Bureau of Investigation.

3. In fulfilling HPSCI’s oversight responsibilities with respect to government intelligence agencies, HPSCI members and staff frequently review information that has been identified as requiring protection from unauthorized disclosure by HPSCI security procedures, Executive Order, the Director of National Intelligence (previously the Director of Central Intelligence), or otherwise by statute. Congressional rules allow HPSCI to hold closed meetings, or executive sessions, when receiving classified or otherwise protected information. Based on my experience with HPSCI, I am familiar with the subject matter of testimony and evidence that HPSCI routinely receives in executive session. Based on my experience with HPSCI, I am also familiar with the types of information that have been identified as requiring protection from unauthorized disclosure as well as markings used by federal agencies to denote information that requires protection from unauthorized disclosure.

4. HPSCI rules in effect during Ms. Roark’s employment stated that Committee staff “shall not . . . discuss or disclose: (A) the classified substance of the work of the Committee; (B) any information received by the Committee in executive session; (C) any classified information received by the Committee from any source; or (D) the substance of any hearing that was closed to the public pursuant to these rules or the Rules of the House.” Rule 12(a)(1), Rules of the Permanent Select Comm. on Intelligence, U.S. House of Representatives, 106th Cong. (1999) (“1999 Committee Rules”). The current HPSCI rules contain substantially similar restrictions.

See Rule 12(a)(1), Rules of the Permanent Select Comm. on Intelligence, U.S. House of Representatives, 113th Cong. (2013) (“2013 Committee Rules”), *available online* <http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/HPSCI%20Rules%20of%20Procedure%20-%20113th%20Congress.pdf>. Attached hereto as Exhibit 1 is a true and correct copy of the Committee Rules for the 106th Congress. Attached hereto as Exhibit 2 is a true and correct copy of the Committee Rules for the 113th Congress.

5. HPSCI rules also required Committee staff to sign non-disclosure agreements “as a condition of employment.” 106th Congress Committee Rule 12(b)(1); *see also* 113th Congress Committee Rule 12(b)(1) (same). Attached hereto as Exhibits 3 and 4 are true and correct copies of non-disclosure agreements signed by plaintiff Diane Roark.

6. Ms. Roark’s non-disclosure agreements required her to “never divulge, publish, or reveal by writing, word, conduct, or otherwise” any:

- “[T]estimony given before the HPSCI in executive session, including the name of any witness who appeared before the HPSCI in executive session,”
- “[M]aterial, restricted data . . . or information received or generated by the HPSCI that has been identified under established HPSCI security procedures, by Executive Order, by the Director of Central Intelligence (DCI), or otherwise by statute, as requiring protection from unauthorized disclosure under and to which [she had] access during [her] tenure with the HPSCI staff,” and
- “Any information classified pursuant to any Executive Order, by the DCI, or otherwise by statute, which might otherwise come into [her] possession.”

(Exhibits 3, 4, ¶¶ 2, 13.). These restrictions applied “during [her] tenure with the HPSCI or anytime thereafter.” *Id.* The agreements also required Ms. Roark “to surrender to the HPSCI . . . upon [her] separation from the HPSCI staff, all information, material, or restricted data” in those categories. (Exs. 3, 4 at ¶ 7).

7. The information referred to in paragraph 2 of Ms. Roark’s NDAs as “information received or generated by HPSCI that has been identified . . . by the Director of Central

Intelligence (DCI) . . . as requiring protection from unauthorized disclosure” includes not only classified information, but also information marked “For Official Use Only,” based on the Director of Central Intelligence’s determination that “For Official Use Only” information required protection from unauthorized disclosure.

8. It is my understanding that the FBI seized various documents/papers and a CD from Ms. Roark. I have conducted a review of a copy of certain paper documents (and some of the contents of the CD) to determine whether the items contain testimony given before the HPSCI in executive session or information received or generated by HPSCI that has been identified as requiring protection from unauthorized disclosure. Based on my experience with HPSCI, I have determined that the following sixteen items contain information that falls within these categories:

Item #	Description (type of item, # of pages, general nature of content)	Basis for HPSCI Claim regarding Document
HC1	9 pages of excerpts of email chains that appear to be from email addresses associated with Ms. Roark, Thomas Drake, Kirk Wiebe, and Edward Loomis; entitled “re: suggestions tonight?”; which appear to date primarily from September 2002	This document describes information received or generated in executive session of the HPSCI, including HPSCI budget information in the classified annex to an intelligence authorization act that the HPSCI adopted in executive session.
HC2	Congressional Staff Visit, 2 pages, dated June 24, 1999.	This document is labeled “Confidential” and thus contains information that has been identified by statute, executive order, or the Director of Central Intelligence as requiring protection from unauthorized disclosure, and it should have been surrendered upon Ms. Roark’s separation from the HPSCI staff.

Item #	Description (type of item, # of pages, general nature of content)	Basis for HPSCI Claim regarding Document
HC3	2 page memorandum for Commander, Naval Security Group, dated April 28, 1999, concerning FY 1999 and 2000 classified annexes.	This document describes information received or generated in executive session of the HPSCI, including HPSCI budget information in the classified annex to an intelligence authorization act that the HPSCI adopted in executive session, and it should have been surrendered upon Ms. Roark's separation from the HPSCI staff.
HC4	Commander Naval Security Group Slides, 18 pages, undated.	This document is labeled "SECRET" and thus contains information that has been identified by statute, executive order, or the Director of Central Intelligence as requiring protection from unauthorized disclosure.
HC5	38 pages of miscellaneous faxes and documents regarding several subjects including HPSCI budget matters, dated June 23, 1998, through August 2, 1999.	<p>This document describes information received or generated in executive session of the HPSCI, including the classified annex to an intelligence authorization act that the HPSCI adopted in executive session, and it should have been surrendered upon Ms. Roark's separation from the HPSCI staff.</p> <p>Some pages of the document are labeled "For Official Use Only" and thus the document also contains information that has been identified by statute, executive order, or the Director of Central Intelligence as requiring protection from unauthorized disclosure.</p>
HC6	23 page Intelligence Review: Audit Report, dated May 8, 1998	This document is marked "For Official Use Only" and thus contains information that has been identified by statute, executive order, or the Director of Central Intelligence as requiring protection from unauthorized disclosure, and it should have been surrendered upon Ms. Roark's separation from the HPSCI staff.

Item #	Description (type of item, # of pages, general nature of content)	Basis for HPSCI Claim regarding Document
HC7	CD of Working Group, dated April 19, 2001	This CD and certain files on the CD are labeled "For Official Use Only" and the CD thus contains information that has been identified by statute, executive order, or the Director of Central Intelligence as requiring protection from unauthorized disclosure, and it should have been surrendered upon Ms. Roark's separation from the HPSCI staff.
HC9	72 page Intelligence Community Information Systems Strategic Plan, dated November 1997	This document is labeled "For Official Use Only" and thus contains information that has been identified by statute, executive order, or the Director of Central Intelligence as requiring protection from unauthorized disclosure, and it should have been surrendered upon Ms. Roark's separation from the HPSCI staff.
HC11	Pre-publication Submission by Diane Roark, 4 pages, undated.	This document contains information that has been identified by statute, executive order, or the Director of Central Intelligence as requiring protection from unauthorized disclosure. The document also describes information received or generated in executive session of the HPSCI.
HC12	Pre-publication Submission by Diane Roark, 4 pages, undated	This document is identical to HC11.
HC13	Pre-publication Submission by Diane Roark, 4 pages, undated	This document is identical to HC11.

Item #	Description (type of item, # of pages, general nature of content)	Basis for HPSCI Claim regarding Document
HC14	5 pages, Initial Comments Regarding Specific Redactions, dated September 11, 2006	<p>This document contains information that has been identified by statute, executive order, or the Director of Central Intelligence as requiring protection from unauthorized disclosure.</p> <p>The document also describes the substance of unspecified congressional testimony, some or all of which may have been executive session testimony before the HPSCI.</p>
HC16	2 page excerpts of emails entitled "Not supposed to make sense", appear to be from email addresses associated with Ms. Roark, and Mr. Drake, undated	This document describes information received or generated in executive session of the HPSCI, including HPSCI budget information in the classified annex to an intelligence authorization act that the HPSCI adopted in executive session.
HC19	1 page excerpt of email entitled "What ethics?", undated (and which may be part of same email exchange as HC 16)	This document describes information received or generated in executive session of the HPSCI, including HPSCI budget information in the classified annex to an intelligence authorization act that the HPSCI adopted in executive session.
HC20	1 page of excerpt of email entitled "...the SSCI and HPSCI authorization language....", dated August 30, 2006.	This document describes information received or generated in executive session of the HPSCI, including HPSCI budget information in the classified annex to an intelligence authorization act that the HPSCI adopted in executive session.

Item #	Description (type of item, # of pages, general nature of content)	Basis for HPSCI Claim regarding Document
HC21	1 page Baseline definition slide, undated	This document is labeled "For Official Use Only" and thus contains information that has been identified by statute, executive order, or the Director of Central Intelligence as requiring protection from unauthorized disclosure. If this document predates Ms. Roark's separation, it should have been surrendered upon Ms. Roark's separation from the HPSCI staff.

9. Based upon my review, it appears that at least six of the foregoing items existed prior to Mr. Roark's retirement from HPSCI and, therefore, should have been surrendered to HPSCI at that time pursuant to paragraph 7 of Ms. Roark's non-disclosure agreement.

10. Based on my review, it appears that all of the foregoing items contain testimony given before the HPSCI in executive session or information received or generated by HPSCI that has been identified as requiring protection from unauthorized disclosure, and, as a result, they should not be returned to Ms. Roark.

11. HPSCI's assertion of interests in the foregoing materials is for the purpose of ensuring that sensitive matters relating to the non-public work of HPSCI are not disclosed. HPSCI has no interest in preserving any of the foregoing materials seized from Ms. Roark. HPSCI is willing to destroy all copies of the foregoing materials in its possession.

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

Executed this 29th day of September 2014 at Washington, D.C.



DARREN M. DICK

CERTIFICATE OF SERVICE

I hereby certify that on September 30, 2014 a copy of the foregoing **Declaration of Darren M. Dick in Support of Defendant's Motion for Summary Judgment** was placed in a postage prepaid envelope and deposited in the United States Mail at Portland, Oregon, addressed to:

Diane Roark
2000 N. Scenic View Dr.
Stayton, OR 97383

And was sent via email to the following email address:

gardenofeden@wvi.com

/s/ James E. Cox, Jr.
JAMES E. COX, JR.

RULES OF PROCEDURE
FOR THE
PERMANENT SELECT COMMITTEE
ON INTELLIGENCE
UNITED STATES HOUSE OF REPRESENTATIVES
106th CONGRESS



(Revised February 1999)

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON : 1999

55-123

H432-1

PERMANENT SELECT COMMITTEE ON INTELLIGENCE

PORTER J. GOSS, Florida, *Chairman*

JERRY LEWIS, California	JULIAN C. DIXON, California
BILL McCOLLUM, Florida	NANCY PELOSI, California
MICHAEL N. CASTLE, Delaware	SANFORD D. BISHOP, Jr., Georgia
SHERWOOD L. BOEHLERT, New York	NORMAN SISISKY, Virginia
CHARLES F. BASS, New Hampshire	GARY A. CONDIT, California
JIM GIBBONS, Nevada	TIM ROEMER, Indiana
RAY LAHOOD, Illinois	ALCEE L. HASTINGS, Florida
HEATHER WILSON, New Mexico	

DENNIS J. HASTERT, Illinois, *Speaker, Ex Officio Member*
RICHARD A. GEPHARDT, Missouri, *Minority Leader, Ex Officio Member*

JOHN I. MILLIS, *Staff Director*
PATRICK B. MURRAY, *Chief Counsel*
MICHAEL W. SHEEHY, *Democratic Counsel*

(II)

CONTENTS

	Page
Rule 1 Subcommittees	1
Rule 2 Regular Meetings of the Full Committee	1
Rule 3 Notice for Meetings	2
Rule 4 Preparations for Committee Meetings	2
Rule 5 Open Meetings	2
Rule 6 Quorum	3
Rule 7 Reporting Record Votes	3
Rule 8 Procedures for Taking Testimony or Receiving Evidence	3
Rule 9 Investigations	6
Rule 10 Subpoenas	7
Rule 11 Committee Staff	7
Rule 12 Limit on Discussion of Classified Work of the Committee	8
Rule 13 Classified Material	10
Rule 14 Procedures Related to Handling Classified Information	10
Rule 15 Legislative Calendar	14
Rule 16 Committee Travel	14
Rule 17 Disciplinary Actions	15
Rule 18 Broadcasting Committee Meetings	16
Rule 19 Committee Records Transferred to National Archives	16
Rule 20 Changes in Rules	16

**RULES OF PROCEDURE FOR THE PERMANENT SELECT COMMITTEE ON
INTELLIGENCE**

1. SUBCOMMITTEES

(a) Generally

(1) Creation of subcommittees shall be by majority vote of the Committee.

(2) Subcommittees shall deal with such legislation and oversight of programs and policies as the Committee may direct.

(3) Subcommittees shall be governed by these rules.

(4) For purposes of these rules, any reference herein to the "Committee" shall be interpreted to include subcommittees, unless otherwise specifically provided.

(b) Establishment of Subcommittees

The Committee establishes the following subcommittees:

(1) Subcommittee on Human Intelligence, Analysis, and Counter-intelligence; and

(2) Subcommittee on Technical and Tactical Intelligence.

(c) Subcommittee Membership

(1) *Generally.*—Each Member of the Committee may be assigned to at least one of the two subcommittees.

(2) *Ex Officio Membership.*—In the event that the Chairman and Ranking Minority Member of the full Committee do not choose to sit as regular voting members of one or both of the subcommittees, each is authorized to sit as an *ex officio* Member of the subcommittees and participate in the work of the subcommittees. When sitting as *ex officio* Members, however, they shall not:

(A) have a vote in the subcommittee;

(B) be counted for purposes of determining a quorum.

2. MEETING DAY

(a) Regular Meeting Day for the Full Committee

(1) *Generally.*—The regular meeting day of the Committee for the transaction of Committee business shall be the first Wednesday of each month, unless otherwise directed by the Chairman.

(2) *Notice Required.*—Such regular business meetings shall not occur unless Members are provided reasonable notice under these rules.

(b) Regular Meeting Day for Subcommittees

There is no regular meeting day for either subcommittee.

(1)

3. NOTICE FOR MEETINGS

(a) Generally

In the case of any meeting of the Committee, the Chief Clerk of the Committee shall provide reasonable notice to every Member of the Committee. Such notice shall provide the time and place of the meeting.

(b) Definition

For purposes of this rule, "reasonable notice" means:

- (1) written notification;
- (2) delivered by facsimile transmission or regular mail, which is:
 - (A) delivered no less than 24 hours prior to the event for which notice is being given, if the event is to be held in Washington, D.C.; or
 - (B) delivered no less than 48 hours prior to the event for which notice is being given, if the event is to be held outside Washington, D.C.

(c) Exception

In extraordinary circumstances only, the Chairman may, after consulting with the Ranking Minority Member, call a meeting of the Committee without providing notice, as defined in subparagraph (b), to Members of the Committee.

4. PREPARATIONS FOR COMMITTEE MEETINGS

(a) Generally

Designated Committee Staff, as directed by the Chairman, shall brief Members of the Committee at a time sufficiently prior to any Committee meeting in order to:

- (1) assist Committee Members in preparation for such meeting; and
- (2) determine which matters Members wish considered during any meeting.

(b) Briefing Materials

- (1) Such a briefing shall, at the request of a Member, include a list of all pertinent papers, and such other materials, that have been obtained by the Committee that bear on matters to be considered at the meeting; and
- (2) The staff director shall also recommend to the Chairman any testimony, papers, or other materials to be presented to the Committee at any meeting of the Committee.

5. OPEN MEETINGS

(a) Generally

Pursuant to Rule XI of the House, but subject to the limitations of subsection (b), Committee meetings held for the transaction of business, and Committee hearings, shall be open to the public.

(b) Exceptions

Any meeting or portion thereof, for the transaction of business, including the markup of legislation, or any hearing or portion thereof, shall be closed to the public, if:

(1) the Committee determines by record vote, in open session with a majority of the Committee present, that the matters to be discussed may:

- (A) endanger national security;
- (B) compromise sensitive law enforcement information;
- (C) tend to defame, degrade, or incriminate any person; or
- (D) otherwise violate any law or Rule of the House.

(2) Notwithstanding paragraph (1), a vote to close a Committee hearing, pursuant to this subsection and House Rule XI shall be taken in open session—

- (A) with a majority of the Committee being present; or
- (B) regardless of whether a majority is present, so long as at least one Member of the Minority is present and votes upon the motion.

(c) Briefings

All Committee briefings shall be closed to the public.

6. QUORUM

(a) Hearings

For purposes of taking testimony, or receiving evidence, a quorum shall consist of two Committee Members.

(b) Other Committee Proceedings

For purposes of the transaction of all other Committee business, other than the consideration of a motion to close a hearing as described in rule 5(b)(2)(B), a quorum shall consist of a majority of Members.

7. REPORTING RECORD VOTES

Whenever the Committee by record vote reports any measure or matter, the report of the Committee upon such measure or matter shall include a tabulation of the votes cast in favor of, and the votes cast in opposition to, such measure or matter.

8. PROCEDURES FOR TAKING TESTIMONY OR RECEIVING EVIDENCE

(a) Notice

Adequate notice shall be given to all witnesses appearing before the Committee.

(b) Oath or Affirmation

The Chairman may require testimony of witnesses to be given under oath or affirmation.

(c) Administration of Oath or Affirmation

Upon the determination that a witness shall testify under oath or affirmation, any Member of the Committee designated by the Chairman may administer the oath or affirmation.

(d) Interrogation of Witnesses

(1) *Generally.*—Interrogation of witnesses before the Committee shall be conducted by Members of the Committee.

(2) *Exception.*—(A) The Chairman, in consultation with the Ranking Minority Member, may determine that Committee Staff will be authorized to question witnesses at a hearing in accordance with clause (2)(j) of House Rule XI.

(B) The Chairman and Ranking Minority Member are each authorized to designate Committee Staff to conduct such questioning.

(e) Counsel for the Witness

(1) *Generally.*—Witnesses before the Committee may be accompanied by counsel, subject to the requirements of paragraph (2).

(2) *Counsel Clearances Required.*—In the event that a meeting of the Committee has been closed because the subject to be discussed deals with classified information, counsel accompanying a witness before the Committee must possess the requisite security clearance and provide proof of such clearance to the Committee at least 24 hours prior to the meeting at which the counsel intends to be present.

(3) *Failure to Obtain Counsel.*—Any witness who is unable to obtain counsel should notify the Committee. If such notification occurs at least 24 hours prior to the witness' appearance before the Committee, the Committee shall then endeavor to obtain voluntary counsel for the witness. Failure to obtain counsel, however, will not excuse the witness from appearing and testifying.

(4) *Conduct of Counsel for Witnesses.*—Counsel for witnesses appearing before the Committee shall conduct themselves ethically and professionally at all times in their dealings with the Committee.

(A) A majority of Members of the Committee may, should circumstances warrant, find that counsel for a witness before the Committee failed to conduct himself or herself in an ethical or professional manner.

(B) Upon such finding, counsel may be subject to appropriate disciplinary action.

(5) *Temporary Removal of Counsel.*—The Chairman may remove counsel during any proceeding before the Committee for failure to act in an ethical and professional manner.

(6) *Committee Reversal.*—A majority of the Members of the Committee may vote to overturn the decision of the Chairman to remove counsel for a witness.

(7) *Role of Counsel for Witness.*—(A) Counsel for a witness:

(i) shall not be allowed to examine witnesses before the Committee, either directly or through cross-examination; but

(ii) may submit questions in writing to the Committee that counsel wishes propounded to a witness; or

(iii) may suggest, in writing to the Committee, the presentation of other evidence or the calling of other witnesses.

(B) The Committee may make such use of any such questions, or suggestions, as the Committee deems appropriate.

(f) Statements by Witnesses

(1) *Generally.*—A witness may make a statement, which shall be brief and relevant, at the beginning and at the conclusion of the witness' testimony.

(2) *Length.*—Each statement shall not exceed five minutes in length, unless otherwise determined by the Chairman.

(3) *Submission to the Committee.*—Any witness desiring to submit a written statement for the record of the proceedings shall submit a copy of the statement to the Chief Clerk of the Committee.

(A) Such statements shall ordinarily be submitted no less than 48 hours in advance of the witness' appearance before the Committee.

(B) In the event that the hearing was called with less than 24 hours notice, written statements should be submitted as soon as practicable prior to the hearing.

(g) Objections and Ruling

(1) *Generally.*—Any objection raised by a witness, or counsel for the witness, shall be ruled upon by the Chairman, and such ruling shall be the ruling of the Committee.

(2) *Committee Action.*—A ruling by the Chairman may be overturned upon a majority vote of the Committee.

(h) Transcripts

(1) *Transcript Required.*—A transcript shall be made of the testimony of each witness appearing before the Committee during any hearing of the Committee.

(2) *Opportunity to Inspect.*—Any witness testifying before the Committee shall be given a reasonable opportunity to inspect the transcript of the hearing, and may be accompanied by counsel to determine whether such testimony was correctly transcribed. Such counsel:

(A) shall have the appropriate clearance necessary to review any classified aspect of the transcript; and

(B) should, to the extent possible, be the same counsel that was present for such classified testimony.

(3) *Corrections.*—(A) Pursuant to Rule XI of the House Rules, any corrections the witness desires to make in a transcript shall be limited to technical, grammatical, and typographical.

(B) Corrections may not be made to change the substance of the testimony.

(C) Such corrections shall be submitted in writing to the Committee within 7 days after the transcript is made available to the witness.

(D) Any questions arising with respect to such corrections shall be decided by the Chairman.

(4) *Copy for the Witness.*—At the request of the witness, any portion of the witness' testimony given in executive session shall be made available to that witness if that testimony is subsequently quoted or intended to be made part of a public record. Such testimony shall be made available to the witness at the witness' expense.

(i) Requests to Testify

(1) *Generally.*—The Committee will consider requests to testify on any matter or measure pending before the Committee.

(2) *Recommendations for Additional Evidence.*—Any person who believes that testimony, other evidence, or commentary, presented at a public hearing may tend to affect adversely that person's reputation may submit to the Committee, in writing:

(A) a request to appear personally before the Committee;

(B) a sworn statement of facts relevant to the testimony, evidence, or commentary; or

(C) proposed questions for the cross-examination of other witnesses.

(3) *Committee's Discretion.*—The Committee may take those actions it deems appropriate with respect to such requests.

(j) Contempt Procedures

Citations for contempt of Congress shall be forwarded to the House, only if:

(1) reasonable notice is provided to all Members of the Committee of a meeting to be held to consider any such contempt recommendations;

(2) the Committee has met and considered the contempt allegations;

(3) the subject of the allegations was afforded an opportunity to state, either in writing or in person, why he or she should not be held in contempt; and

(4) the Committee agreed by majority vote to forward the citation recommendations to the House.

(k) Release of Name of Witness

(1) *Generally.*—At the request of a witness scheduled to be heard by the Committee, the name of that witness shall not be released publicly prior to, or after, the witness' appearance before the Committee.

(2) *Exception.*—Notwithstanding paragraph (1), the Chairman may authorize the release to the public of the name of any witness scheduled to appear before the Committee.

9. INVESTIGATIONS

(a) Commencing Investigations

(1) *Generally.*—The Committee shall conduct investigations only if approved by the full Committee. An investigation may be initiated either:

(A) by a vote of the full Committee;

(B) at the direction of the Chairman of the full Committee, with notice to the Ranking Minority Member; or

(C) by written request of at least five Members of the full Committee, which is submitted to the Chairman.

(2) *Full Committee Ratification Required.*—Any investigation initiated by the Chairman pursuant to paragraphs (B) and (C) must be brought to the attention of the full Committee for approval, at the next regular meeting of the full Committee.

(b) Conducting Investigations

An authorized investigation may be conducted by: (1) Members of the Committee; or (2) Committee Staff members designated by the Chairman, in consultation with the Ranking Minority Member.

10. SUBPOENAS

(a) Generally

All subpoenas shall be authorized by the Chairman of the full Committee, upon consultation with the Ranking Minority Member, or by vote of the Committee.

(b) Subpoena Contents

Any subpoena authorized by the Chairman of the full Committee, or the Committee, may compel:

- (1) the attendance of witnesses and testimony before the Committee; or
- (2) the production of memoranda, documents, records, or any other tangible item.

(c) Signing of Subpoenas

A subpoena authorized by the Chairman of the full Committee, or the Committee, may be signed by the Chairman, or by any Member of the Committee designated to do so by the Committee.

(d) Subpoena Service

A subpoena authorized by the Chairman of the full Committee, or the Committee, may be served by any person designated to do so by the Chairman.

(e) Other Requirements

Each subpoena shall have attached thereto a copy of these rules.

11. COMMITTEE STAFF

(a) Definition

For the purpose of these rules, "Committee Staff" or "staff of the Committee" means:

- (1) employees of the Committee;
- (2) consultants to the Committee;
- (3) employees of other Government agencies detailed to the Committee; or
- (4) any other person engaged by contract, or otherwise, to perform services for, or at the request of, the Committee.

(b) Appointment of Committee Staff

(1) *Chairman's Authority.*—The appointment of Committee Staff shall be by the Chairman, in consultation with the Ranking Minority Member. The Chairman shall certify Committee Staff appointments to the Clerk of the House in writing.

(2) *Security Clearance Required.*—All offers of employment for prospective Committee Staff positions shall be contingent upon:

- (A) the results of a background investigation; and

(B) a determination by the Chairman that requirements for the appropriate security clearances have been met.

(c) Responsibilities of Committee Staff

(1) *Generally.*—The Committee Staff works for the Committee as a whole, under the supervision and direction of the Chairman of the Committee.

(2) *Authority of the Staff Director.*—(A) Unless otherwise determined by the Committee, the duties of Committee Staff shall be performed under the direct supervision and control of the staff director.

(B) Committee Staff personnel affairs and day-to-day Committee Staff administrative matters, including the security and control of classified documents and material, shall be administered under the direct supervision and control of the staff director.

(3) *Staff Assistance to Minority Membership.*—The Committee Staff shall assist the Minority as fully as the Majority of the Committee in all matters of Committee business, and in the preparation and filing of supplemental, minority, or additional views, to the end that all points of view may be fully considered by the Committee and the House.

12. LIMIT ON DISCUSSION OF CLASSIFIED WORK OF THE COMMITTEE

(a) Prohibition

(1) *Generally.*—Except as otherwise provided by these rules and the Rules of the House, Members and Committee Staff shall not at any time, either during that person's tenure as a Member of the Committee or as Committee Staff, or anytime thereafter, discuss or disclose:

(A) the classified substance of the work of the Committee;

(B) any information received by the Committee in executive session;

(C) any classified information received by the Committee from any source; or

(D) the substance of any hearing that was closed to the public pursuant to these rules or the Rules of the House.

(2) *Non-Disclosure in Proceedings.*—(A) Members of the Committee and the Committee Staff shall not discuss either the substance or procedure of the work of the Committee with any person not a Member of the Committee or the Committee Staff in connection with any proceeding, judicial or otherwise, either during the person's tenure as a Member of the Committee, or of the Committee Staff, or at any time thereafter, except as directed by the Committee in accordance with the Rules of the House and these rules.

(B) In the event of the termination of the Committee, Members and Committee Staff shall be governed in these matters in a manner determined by the House concerning discussions of the classified work of the Committee.

(3) *Exceptions.*—(A) Notwithstanding the provisions of subsection (a)(1), Members of the Committee and the Committee Staff may

discuss and disclose those matters described in subsection (a)(1) with:

(i) Members and staff of the Senate Select Committee on Intelligence designated by the chairman of that committee;

(ii) the chairmen and ranking minority members of the House and Senate Committees on Appropriations and staff of those committees designated by the chairmen of those committees; and

(iii) the chairman and ranking minority member of the Subcommittee on National Security of the House Committee on Appropriations and staff of that subcommittee as designated by the chairman of that subcommittee.

(B) Notwithstanding the provisions of subsection (a)(1), Members of the Committee and the Committee Staff may discuss and disclose only that budget-related information necessary to facilitate the enactment of the annual defense authorization bill with the chairmen and ranking minority members of the House and Senate Committees on Armed Services and the staff of those committees designated by the chairmen of those committees.

(C) Members and Committee Staff may discuss and disclose such matters as otherwise directed by the Committee.

(b) Non-Disclosure Agreement

(1) *Generally.*—All Committee Staff must, before joining the Committee, agree in writing, as a condition of employment, not to divulge any classified information, which comes into such person's possession while a member of the Committee Staff, to any person not a Member of the Committee or the Committee Staff, except as authorized by the Committee in accordance with the Rules of the House and these rules.

(2) *Other Requirements.*—In the event of the termination of the Committee, Members and Committee Staff must follow any determination by the House of Representatives, with respect to the protection of classified information received while a Member of the Committee or as Committee Staff.

(3) *Requests for Testimony of Staff.*—(A) All Committee Staff must, as a condition of employment, agree in writing, to notify the Committee immediately of any request for testimony received while a member of the Committee Staff, or at any time thereafter, concerning any classified information received by such person while a member of the Committee Staff.

(B) Committee Staff shall not disclose, in response to any such request for testimony, any such classified information, except as authorized by the Committee in accordance with the Rules of the House and these rules.

(C) In the event of the termination of the Committee, Committee Staff will be subject to any determination made by the House of Representatives with respect to any requests for testimony involving classified information received while a member of the Committee Staff.

13. CLASSIFIED MATERIAL

(a) Receipt of Classified Information

(1) *Generally.*—In the case of any information that has been classified under established security procedures and submitted to the Committee by any source, the Committee shall receive such classified information as executive session material.

(2) *Staff Receipt of Classified Materials.*—For purposes of receiving classified information, the Committee Staff is authorized to accept information on behalf of the Committee.

(b) Non-Disclosure of Classified Information

Any classified information received by the Committee, from any source, shall not be disclosed to any person not a Member of the Committee or the Committee Staff, or otherwise released, except as authorized by the Committee in accord with the Rules of the House and these rules.

14. PROCEDURES RELATED TO HANDLING OF CLASSIFIED INFORMATION

(a) Security Measures

(1) *Strict Security.*—The Committee's offices shall operate under strict security procedures administered by the Director of Security and Registry of the Committee under the direct supervision of the staff director.

(2) *U.S. Capitol Police Presence Required.*—At least one U.S. Capitol Police officer shall be on duty at all times outside the entrance to Committee offices to control entry of all persons to such offices.

(3) *Identification Required.*—Before entering the Committee's offices all persons shall identify themselves to the U.S. Capitol Police officer described in paragraph (2) and to a Member of the Committee or Committee Staff.

(4) *Maintenance of Classified Materials.*—Classified documents shall be segregated and maintained in approved security storage locations.

(5) *Examination of Classified Materials.*—Classified documents in the Committee's possession shall be examined in an appropriately secure manner.

(6) *Prohibition on Removal of Classified Materials.*—Removal of any classified document from the Committee's offices is strictly prohibited, except as provided by these rules.

(7) *Exception.*—Notwithstanding the prohibition set forth in paragraph (6), a classified document, or copy thereof, may be removed from the Committee's offices in furtherance of official Committee business. Appropriate security procedures shall govern the handling of any classified documents removed from the Committee's offices.

(b) Access to Classified Information by Members

All Members of the Committee shall at all times have access to all classified papers and other material received by the Committee from any source.

(c) Need-to-know

(1) *Generally.*—Committee Staff shall have access to any classified information provided to the Committee on a strict “need-to-know” basis, as determined by the Committee, and under the Committee’s direction by the staff director.

(2) *Appropriate Clearances Required.*—Committee Staff must have the appropriate clearances prior to any access to compartmented information.

(d) Oath

(1) *Requirement.*—Before any Member of the Committee, or the Committee Staff, shall have access to classified information, the following oath shall be executed:

I do solemnly swear (or affirm) that I will not disclose any classified information received in the course of my service on the House Permanent Select Committee on Intelligence, except when authorized to do so by the Committee or the House of Representatives.

(2) *Copy.*—A copy of such executed oath shall be retained in the files of the Committee.

(e) Registry

(1) *Generally.*—The Committee shall maintain a registry that:

(A) provides a brief description of the content of all classified documents provided to the Committee by the executive branch that remain in the possession of the Committee; and

(B) lists by number all such documents.

(2) *Designation by the Staff Director.*—The staff director shall designate a member of the Committee Staff to be responsible for the organization and daily maintenance of such registry.

(3) *Availability.*—Such registry shall be available to all Members of the Committee and Committee Staff.

(f) Requests by Members of Other Committees

Pursuant to the Rules of the House, Members who are not Members of the Committee may be granted access to such classified transcripts, records, data, charts, or files of the Committee, and be admitted on a non-participatory basis to classified hearings of the Committee involving discussions of classified material in the following manner:

(1) *Written Notification Required.*—Members who desire to examine classified materials in the possession of the Committee, or to attend Committee hearings or briefings on a non-participatory basis, must notify the Chief Clerk of the Committee in writing.

(2) *Committee Consideration.*—The Committee shall consider each such request by non-Committee Members at the earliest practicable opportunity. The Committee shall determine, by roll call vote, what action it deems appropriate in light of all of the circumstances of each request. In its determination, the Committee shall consider:

(A) the sensitivity to the national defense or the confidential conduct of the foreign relations of the United States of the information sought;

(B) the likelihood of its being directly or indirectly disclosed;
 (C) the jurisdictional interest of the Member making the request; and

(D) such other concerns, constitutional or otherwise, as may affect the public interest of the United States.

(3) *Committee Action.*—After consideration of the Member's request, the Committee may take any action it may deem appropriate under the circumstances, including but not limited to:

(A) approving the request, in whole or part;

(B) denying the request; or

(C) providing the requested information or material in a different form than that sought by the Member.

(4) *Consultation Authorized.*—When considering a Member's request, the Committee may consult the Director of Central Intelligence and such other officials it considers necessary.

(5) *Finality of Committee Decision.*—(A) Should the Member making such a request disagree with the Committee's determination with respect to that request, or any part thereof, that Member must notify the Committee in writing of such disagreement.

(B) The Committee shall subsequently consider the matter and decide, by record vote, what further action or recommendation, if any, the Committee will take.

(g) Advising the House or Other Committees

Pursuant to Section 501 of the National Security Act of 1947 (50 U.S.C. §413), and to the Rules of the House, the Committee shall call to the attention of the House, or to any other appropriate committee of the House, those matters requiring the attention of the House, or such other committee, on the basis of the following provisions:

(1) *By Request of Committee Member.*—At the request of any Member of the Committee to call to the attention of the House, or any other committee, executive session material in the Committee's possession, the Committee shall meet at the earliest practicable opportunity to consider that request.

(2) *Committee Consideration of Request.*—The Committee shall consider the following factors, among any others it deems appropriate:

(A) the effect of the matter in question on the national defense or the foreign relations of the United States;

(B) whether the matter in question involves sensitive intelligence sources and methods;

(C) whether the matter in question otherwise raises serious questions affecting the national interest; and

(D) whether the matter in question affects matters within the jurisdiction of another Committee of the House.

(3) *Views of Other Committees.*—In examining such factors, the Committee may seek the opinion of Members of the Committee appointed from standing committees of the House with jurisdiction over the matter in question, or submissions from such other committees.

(4) *Other Advice.*—The Committee may, during its deliberations on such requests, seek the advice of any executive branch official.

(h) Reasonable Opportunity to Examine Materials

Before the Committee makes any decision regarding any request for access to any classified information in its possession, or a proposal to bring any matter to the attention of the House or another committee, Members of the Committee shall have a reasonable opportunity to examine all pertinent testimony, documents, or other materials in the Committee's possession that may inform their decision on the question.

(i) Notification to the House

The Committee may bring a matter to the attention of the House when, after consideration of the factors set forth in this rule, it considers the matter in question so grave that it requires the attention of all Members of the House, and time is of the essence, or for any reason the Committee finds compelling.

(j) Method of Disclosure to the House

(1) Should the Committee decide by roll call vote that a matter requires the attention of the House as described in subsection (i), it shall make arrangements to notify the House promptly.

(2) In such cases, the Committee shall consider whether:

(A) to request an immediate secret session of the House (with time equally divided between the Majority and the Minority); or

(B) to publicly disclose the matter in question pursuant to clause 11(g) of House Rule X.

(k) Requirement to Protect Sources and Methods

In bringing a matter to the attention of the House, or another committee, the Committee, with due regard for the protection of intelligence sources and methods, shall take all necessary steps to safeguard materials or information relating to the matter in question.

(l) Availability of Information to Other Committees

The Committee, having determined that a matter shall be brought to the attention of another committee, shall ensure that such matter, including all classified information related to that matter, is promptly made available to the chairman and ranking minority member of such other committee.

(m) Provision of Materials

The Director of Security and Registry for the Committee shall provide a copy of these rules, and the applicable portions of the Rules of the House governing the handling of classified information, along with those materials determined by the Committee to be made available to such other committee of the House.

(n) Ensuring Clearances and Secure Storage

The Director of Security and Registry for the Committee shall ensure that such other committee or Member (not a Member of the Committee) receiving such classified materials may properly store classified materials in a manner consistent with all governing rules, regulations, policies, procedures, and statutes.

(o) Log

The Director of Security and Registry for the Committee shall maintain a written record identifying the particular classified document or material provided to such other committee or Member (not a Member of the Committee), the reasons agreed upon by the Committee for approving such transmission, and the name of the committee or Member (not a Member of the Committee) receiving such document or material.

(p) Miscellaneous Requirements

(1) *Staff Director's Additional Authority.*—The staff director is further empowered to provide for such additional measures, which he or she deems necessary, to protect such classified information authorized by the Committee to be provided to such other committee or Member (not a Member of the Committee).

(2) *Notice to Originating Agency.*—In the event that the Committee authorizes the disclosure of classified information provided to the Committee by an agency of the executive branch to a Member (not a Member of the Committee) or to another committee, the Chairman may notify the providing agency of the Committee's action prior to the transmission of such classified information.

15. LEGISLATIVE CALENDAR

(a) Generally

The Chief Clerk of the Committee, under the direction of the staff director, shall maintain a printed calendar that lists:

- (1) the legislative measures introduced and referred to the Committee;
- (2) the status of such measures; and
- (3) such other matters that the Committee may require.

(b) Revisions to the Calendar

The calendar shall be revised from time to time to show pertinent changes.

(c) Availability

A copy of each such revision shall be furnished to each Member, upon request.

(d) Consultation with Appropriate Government Entities

Unless otherwise directed by the Committee, legislative measures referred to the Committee shall be referred by the Chief Clerk of the Committee to the appropriate department or agency of the Government for reports thereon.

16. COMMITTEE TRAVEL

(a) Authority

The Chairman may authorize Members and Committee Staff to travel on Committee business.

(b) Requests

(1) *Member Requests.*—Members requesting authorization for such travel shall state the purpose and length of the trip, and shall submit such request directly to the Chairman.

(2) *Committee Staff Requests.*—Committee Staff requesting authorization for such travel shall state the purpose and length of the trip, and shall submit such request through their supervisors to the staff director and the Chairman.

(c) Notification to Members

(1) *Generally.*—Members shall be notified of all foreign travel of Committee Staff not accompanying a Member.

(2) *Content.*—All Members are to be advised, prior to the commencement of such travel, of its length, nature, and purpose.

(d) Trip Reports

(1) *Generally.*—A full report of all issues discussed during any Committee travel shall be submitted to the Chief Clerk of the Committee within a reasonable period of time following the completion of such trip.

(2) *Availability of Reports.*—Such report shall be:

(A) available for the review of any Member or Committee Staff; and

(B) considered executive session material for purposes of these rules.

(e) Limitations on Travel

(1) *Generally.*—The Chairman is not authorized to permit travel on Committee business of Committee Staff who have not satisfied the requirements of subsection (d) of this rule.

(2) *Exception.*—The Chairman may authorize Committee Staff to travel on Committee business, notwithstanding the requirements of subsections (d) and (e) of this rule—

(A) at the specific request of a Member of the Committee; or

(B) in the event there are circumstances beyond the control of the Committee Staff hindering compliance with such requirements.

(f) Definitions

For purposes of this rule the term “reasonable period of time” means:

(1) no later than 60 days after returning from a foreign trip;

and

(2) no later than 30 days after returning from a domestic trip.

17. DISCIPLINARY ACTIONS

(a) Generally

The Committee shall immediately consider whether disciplinary action shall be taken in the case of any member of the Committee Staff alleged to have failed to conform to any Rule of the House or to these rules.

(b) Exception

In the event the House of Representatives is:

- (1) in a recess period in excess of 3 days; or
- (2) has adjourned *sine die*;

the Chairman of the full Committee, in consultation with the Ranking Minority Member, may take such immediate disciplinary actions deemed necessary.

(c) Available Actions

Such disciplinary action may include immediate dismissal from the Committee Staff.

(d) Notice to Members

All Members shall be notified as soon as practicable, either by facsimile transmission or regular mail, of any disciplinary action taken by the Chairman pursuant to subsection (b).

(e) Reconsideration of Chairman's Actions

A majority of the Members of the full Committee may vote to overturn the decision of the Chairman to take disciplinary action pursuant to subsection (b).

18. BROADCASTING COMMITTEE MEETINGS

Whenever any hearing or meeting conducted by the Committee is open to the public, a majority of the Committee may permit that hearing or meeting to be covered, in whole or in part, by television broadcast, radio broadcast, and still photography, or by any of such methods of coverage, subject to the provisions and in accordance with the spirit of the purposes enumerated in the Rules of the House.

19. COMMITTEE RECORDS TRANSFERRED TO THE NATIONAL ARCHIVES

(a) Generally

The records of the Committee at the National Archives and Records Administration shall be made available for public use in accordance with the Rules of the House.

(b) Notice of Withholding

The Chairman shall notify the Ranking Minority Member of any decision, pursuant to the Rules of the House, to withhold a record otherwise available, and the matter shall be presented to the full Committee for a determination of the question of public availability on the written request of any Member of the Committee.

20. CHANGES IN RULES

(a) Generally

These rules may be modified, amended, or repealed by vote of the full Committee.

(b) Notice of Proposed Changes

A notice, in writing, of the proposed change shall be given to each Member at least 48 hours prior to any meeting at which action on the proposed rule change is to be taken.

○

CHAIRMAN’S MARK

**RULES OF PROCEDURE
FOR THE PERMANENT SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES HOUSE OF REPRESENTATIVES
113TH CONGRESS**

1. MEETING DAY

Regular Meeting Day for the Full Committee. The regular meeting day of the Committee for the transaction of Committee business shall be the first Thursday of each month, unless otherwise directed by the Chair.

2. NOTICE FOR MEETINGS

(a) Generally. In the case of any meeting of the Committee, the Chief Clerk of the Committee shall provide reasonable notice to every member of the Committee. Such notice shall provide the time, place, and subject matter of the meeting, and shall be made consistent with the provisions of clause 2(g)(3) of House Rule XI.

(b) Hearings. Except as provided in subsection (d), a Committee hearing may not commence earlier than one week after such notice.

(c) Business Meetings. Except as provided in subsection (d), a Committee business meeting may not commence earlier than the third day on which Members have notice thereof.

(d) Exception. A hearing or business meeting may begin sooner than otherwise specified in either of the following circumstances (in which case the Chair shall provide the notice at the earliest possible time):

(1) the Chair, with the concurrence of the Ranking Minority Member, determines there is good cause; or

(2) the Committee so determines by majority vote in the presence of the number of members required under the rules of the committee for the transaction of business.

(e) Definition. For purposes of this rule, “notice” means:

(1) Written notification; or

(2) Notification delivered by facsimile transmission, regular mail, or electronic mail.

3. PREPARATIONS FOR COMMITTEE MEETINGS

(a) Generally. Designated Committee Staff, as directed by the Chair, shall brief members of the Committee at a time sufficiently prior to any Committee meeting in order to:

- (1) Assist Committee members in preparation for such meeting; and
 - (2) Determine which matters members wish considered during any meeting.
- (b) Briefing Materials.
- (1) Such a briefing shall, at the request of a member, include a list of all pertinent papers, and such other materials, that have been obtained by the Committee that bear on matters to be considered at the meeting; and
 - (2) The Staff Director shall also recommend to the Chair any testimony, papers, or other materials to be presented to the Committee at the meeting of the Committee.

4. OPEN MEETINGS

- (a) Generally. Pursuant to House Rule XI, but subject to the limitations of subsections (b) and (c), Committee meetings held for the transaction of business and Committee hearings shall be open to the public.
- (b) Meetings. Any meeting or portion thereof, for the transaction of business, including the markup of legislation, or any hearing or portion thereof, shall be closed to the public, if the Committee determines by record vote in open session, with a majority of the Committee present, that disclosure of the matters to be discussed may:
- (1) Endanger national security;
 - (2) Compromise sensitive law enforcement information;
 - (3) Tend to defame, degrade, or incriminate any person; or
 - (4) Otherwise violate any law or Rule of the House.
- (c) Hearings. The Committee may vote to close a Committee hearing pursuant to clause 11(d)(2) of House Rule X, regardless of whether a majority is present, so long as at least two members of the Committee are present, one of whom is a member of the Minority and votes upon the motion.
- (d) Briefings. Committee briefings shall be closed to the public.

5. QUORUM

- (a) Hearings. For purposes of taking testimony, or receiving evidence, a quorum shall consist of two Committee members, at least one of whom is a member of the Majority.
- (b) Other Committee Proceedings. For purposes of the transaction of all other Committee business, other than the consideration of a motion to close a hearing as described in rule 4(c), a quorum shall consist of a majority of members.

6. PROCEDURES FOR AMENDMENTS AND VOTES

- (a) Amendments. When a bill or resolution is being considered by the Committee, members shall provide the Chief Clerk in a timely manner with a sufficient number of written copies of any amendment offered, so as to enable each member present to receive a copy thereof prior to taking action. A point of order may be made against

any amendment not reduced to writing. A copy of each such amendment shall be maintained in the public records of the Committee.

(b) Reporting Record Votes. Whenever the Committee reports any measure or matter by record vote, the report of the Committee upon such measure or matter shall include a tabulation of the votes cast in favor of, and the votes cast in opposition to, such measure or matter.

(c) Postponement of Further Proceedings. In accordance with clause 2(h) of House Rule XI, the Chair is authorized to postpone further proceedings when a record vote is ordered on the question of approving a measure or matter or adopting an amendment. The Chair may resume proceedings on a postponed request at any time after reasonable notice. When proceedings resume on a postponed question, notwithstanding any intervening order for the previous question, an underlying proposition shall remain subject to further debate or amendment to the same extent as when the question was postponed.

(d) Availability of Record Votes on Committee Website. In addition to any other requirement of the Rules of the House, the Chair shall make the record votes on any measure or matter on which a record vote is taken, other than a motion to close a Committee hearing, briefing, or meeting, available on the Committee's website not later than 2 business days after such vote is taken. Such record shall include an unclassified description of the amendment, motion, order, or other proposition, the name of each member voting in favor of, and each member voting in opposition to, such amendment, motion, order, or proposition, and the names of those members of the Committee present but not voting.

7. SUBCOMMITTEES

(a) Generally.

- (1) Creation of subcommittees shall be by majority vote of the Committee.
- (2) Subcommittees shall deal with such legislation and oversight of programs and policies as the Committee may direct.
- (3) Subcommittees shall be governed by these rules.
- (4) For purposes of these rules, any reference herein to the "Committee" shall be interpreted to include subcommittees, unless otherwise specifically provided.

(b) Establishment of Subcommittees. The Committee establishes the following subcommittees:

- (1) Subcommittee on Terrorism, Human Intelligence, Analysis, and Counterintelligence;
- (2) Subcommittee on Technical and Tactical Intelligence; and,
- (3) Subcommittee on Oversight and Investigations.

(c) Subcommittee Membership.

- (1) Generally. Each member of the Committee may be assigned to at least one of the subcommittees.

(2) *Ex Officio* Membership. In the event that the Chair and Ranking Minority Member of the full Committee do not choose to sit as regular voting members of one or more of the subcommittees, each is authorized to sit as an *ex officio* member of the subcommittees and participate in the work of the subcommittees. When sitting *ex officio*, however, they:

(A) Shall not have a vote in the subcommittee; and

(B) Shall not be counted for purposes of determining a quorum.

(d) Regular Meeting Day for Subcommittees. There is no regular meeting day for subcommittees.

8. PROCEDURES FOR TAKING TESTIMONY OR RECEIVING EVIDENCE

(a) Notice. Adequate notice shall be given to all witnesses appearing before the Committee.

(b) Oath or Affirmation. The Chair may require testimony of witnesses to be given under oath or affirmation.

(c) Administration of Oath or Affirmation. Upon the determination that a witness shall testify under oath or affirmation, any member of the Committee designated by the Chair may administer the oath or affirmation.

(d) Questioning of Witnesses.

(1) Generally. Questioning of witnesses before the Committee shall be conducted by members of the Committee.

(2) Exceptions.

(A) The Chair, in consultation with the Ranking Minority Member, may determine that Committee Staff will be authorized to question witnesses at a hearing in accordance with clause (2)(j) of House Rule XI.

(B) The Chair and Ranking Minority Member are each authorized to designate Committee Staff to conduct such questioning.

(e) Counsel for the Witness.

(1) Generally. Witnesses before the Committee may be accompanied by counsel, subject to the requirements of paragraph (2).

(2) Counsel Clearances Required. In the event that a meeting of the Committee has been closed because the subject to be discussed deals with classified information, counsel accompanying a witness before the Committee must possess the requisite security clearance and provide proof of such clearance to the Committee at least 24 hours prior to the meeting at which the counsel intends to be present.

(3) Failure to Obtain Counsel. Any witness who is unable to obtain counsel should notify the Committee. If such notification occurs at least 24 hours prior to the witness' appearance before the Committee, the Committee shall then endeavor to obtain voluntary counsel for the witness. Failure to obtain counsel, however, will not excuse the witness from appearing and testifying.

(4) Conduct of Counsel for Witnesses. Counsel for witnesses appearing before the Committee shall conduct themselves ethically and professionally at all times in their dealings with the Committee.

(A) A majority of members of the Committee may, should circumstances warrant, find that counsel for a witness before the Committee failed to conduct himself or herself in an ethical or professional manner.

(B) Upon such finding, counsel may be subject to appropriate disciplinary action.

(5) Temporary Removal of Counsel. The Chair may remove counsel during any proceeding before the Committee for failure to act in an ethical and professional manner.

(6) Committee Reversal. A majority of the members of the Committee may vote to overturn the decision of the Chair to remove counsel for a witness.

(7) Role of Counsel for Witness.

(A) Counsel for a witness:

(i) Shall not be allowed to examine witnesses before the Committee, either directly or through cross-examination; but

(ii) May submit questions in writing to the Committee that counsel wishes propounded to a witness; or

(iii) May suggest, in writing to the Committee, the presentation of other evidence or the calling of other witnesses.

(B) The Committee may make such use of any such questions, or suggestions, as the Committee deems appropriate.

(f) Statements by Witnesses.

(1) Generally. A witness may make a statement, which shall be brief and relevant, at the beginning and at the conclusion of the witness' testimony.

(2) Length. Each such statement shall not exceed five minutes in length, unless otherwise determined by the Chair.

(3) Submission to the Committee. Any witness desiring to submit a written statement for the record of the proceeding shall submit a copy of the statement to the Chief Clerk of the Committee.

(A) Such statements shall ordinarily be submitted no less than 48 hours in advance of the witness' appearance before the Committee and shall be submitted in written and electronic format.

(B) In the event that the hearing was called with less than 24 hours notice, written statements should be submitted as soon as practicable prior to the hearing.

(g) Objections and Ruling.

(1) Generally. Any objection raised by a witness, or counsel for the witness, shall be ruled upon by the Chair, and such ruling shall be the ruling of the Committee.

(2) Committee Action. A ruling by the Chair may be overturned upon a majority vote of the Committee.

(h) Transcripts.

(1) Transcript Required. A transcript shall be made of the testimony of each witness appearing before the Committee during any hearing of the Committee.

(2) Opportunity to Inspect. Any witness testifying before the Committee shall be given a reasonable opportunity to inspect the transcript of the hearing, and may be accompanied by counsel to determine whether such testimony was correctly transcribed. Such counsel:

(A) May review the transcript only if he or she has the appropriate security clearances necessary to review any classified aspect of the transcript; and

(B) Should, to the extent possible, be the same counsel that was present for such classified testimony.

(3) Corrections.

(A) Pursuant to Rule XI of the House Rules, any corrections the witness desires to make in a transcript shall be limited to technical, grammatical, and typographical corrections.

(B) Corrections may not be made to change the substance of the testimony.

(C) Such corrections shall be submitted in writing to the Committee within 7 days after the transcript is made available to the witnesses.

(D) Any questions arising with respect to such corrections shall be decided by the Chair.

(4) Copy for the Witness. At the request of the witness, any portion of the witness' testimony given in executive session shall be made available to that witness if that testimony is: subsequently quoted or intended to be made part of a public record. Such testimony shall be made available to the witness at the witness' expense.

(i) Requests to Testify.

(1) Generally. The Committee will consider requests to testify on any matter or measure pending before the Committee.

(2) Recommendations for Additional Evidence. Any person who believes that testimony, other evidence, or commentary, presented at a public hearing may tend to affect adversely that person's reputation may submit to the Committee, in writing:

(A) A request to appear personally before the Committee;

(B) A sworn statement of facts relevant to the testimony, evidence, or commentary; or

(C) Proposed questions for the cross-examination of other witnesses.

(3) Committee Discretion. The Committee may take those actions it deems appropriate with respect to such requests.

(j) Contempt Procedures. Citations for contempt of Congress shall be forwarded to the House only if:

(1) Reasonable notice is provided to all members of the Committee of a meeting to be held to consider any such contempt recommendations;

(2) The Committee has met and considered the contempt allegations;

(3) The subject of the allegations was afforded an opportunity to state either in writing or in person, why he or she should not be held in contempt; and

(4) The Committee agreed by majority vote to forward the citation recommendations to the House.

(k) Release of Name of Witness.

(1) Generally. At the request of a witness scheduled to be heard by the Committee, the name of that witness shall not be released publicly prior to, or after, the witness' appearance before the Committee.

(2) Exceptions. Notwithstanding paragraph (1), the Chair may authorize the release to the public of the name of any witness scheduled to appear before the Committee.

9. INVESTIGATIONS

(a) Commencing Investigations. The Committee shall conduct investigations only if approved by the Chair, in consultation with the Ranking Minority Member.

(b) Conducting Investigations. An authorized investigation may be conducted by members of the Committee or Committee Staff designated by the Chair, in consultation with the Ranking Minority Member, to undertake any such investigation.

10. SUBPOENAS

(a) Generally. All subpoenas shall be authorized by the Chair of the full Committee, upon consultation with the Ranking Minority Member, or by vote of the Committee.

(b) Subpoena Contents. Any subpoena authorized by the Chair of the full Committee, or the Committee, may compel:

(1) The attendance of witnesses and testimony before the Committee; or

(2) The production of memoranda, documents, records, or any other tangible item.

(c) Signing of Subpoena. A subpoena authorized by the Chair of the full Committee, or the Committee, may be signed by the Chair, or by any member of the Committee designated to do so by the Committee.

(d) Subpoena Service. A subpoena authorized by the Chair of the full Committee, or the Committee, may be served by any person designated to do so by the Chair.

(e) Other Requirements. Each subpoena shall have attached thereto a copy of these rules.

11. COMMITTEE STAFF

(a) Definition. For the purpose of these rules, “Committee Staff” or “Staff of the Committee” means:

- (1) Employees of the Committee;
- (2) Consultants to the Committee;
- (3) Employees of other Government agencies detailed to the Committee; or
- (4) Any other person engaged by contract, or otherwise, to perform services for, or at the request of, the Committee.

(b) Appointment of Committee Staff and Security Requirements.

- (1) Chair’s Authority. Except as provided in paragraph (2), the Committee Staff shall be appointed, and may be removed, by the Chair and shall work under the general supervision and direction of the Chair.
- (2) Staff Assistance to Minority Membership. Except as provided in paragraphs (3) and (4), and except as otherwise provided by Committee Rules, the Committee Staff provided to the Minority Party members of the Committee shall be appointed, and may be removed, by the Ranking Minority Member of the Committee, and shall work under the general supervision and direction of such member.
- (3) Security Clearance Required. All offers of employment for prospective Committee Staff positions shall be contingent upon:
 - (A) The results of a background investigation; and
 - (B) A determination by the Chair that requirements for the appropriate security clearances have been met.
- (4) Security Requirements. Notwithstanding paragraph (2), the Chair shall supervise and direct the Committee Staff with respect to the security and nondisclosure of classified information. Committee Staff shall comply with requirements necessary to ensure the security and nondisclosure of classified information as determined by the Chair in consultation with the Ranking Minority Member.

12. LIMIT ON DISCUSSION OF CLASSIFIED WORK OF THE COMMITTEE

(a) Prohibition.

- (1) Generally. Except as otherwise provided by these rules and the Rules of the House of Representatives, members of the Committee and Committee Staff shall not at any time, either during that person’s tenure as a member of

the Committee or as Committee Staff, or anytime thereafter, discuss or disclose, or cause to be discussed or disclosed:

- (A) The classified substance of the work of the Committee;
- (B) Any information received by the Committee in executive session;
- (C) Any classified information received by the Committee from any source; or
- (D) The substance of any hearing that was closed to the public pursuant to these rules or the Rules of the House.

(2) Non-Disclosure in Proceedings.

(A) Members of the Committee and the Committee Staff shall not discuss either the substance or procedure of the work of the Committee with any person not a member of the Committee or the Committee Staff in connection with any proceeding, judicial or otherwise, either during the person's tenure as a member of the Committee, or of the Committee Staff, or at any time thereafter, except as directed by the Committee in accordance with the Rules of the House and these rules.

(B) In the event of the termination of the Committee, members and Committee Staff shall be governed in these matters in a manner determined by the House concerning discussions of the classified work of the Committee.

(3) Exceptions.

(A) Notwithstanding the provisions of subsection (a)(1), members of the Committee and the Committee Staff may discuss and disclose those matters described in subsection (a)(1) with:

- (i) Members and staff of the Senate Select Committee on Intelligence designated by the chair of that committee;
- (ii) The chairmen and ranking minority members of the House and Senate Committees on Appropriations and staff of those committees designated by the chairmen of those committees; and,
- (iii) The chair and ranking minority member of the Subcommittee on Defense of the House Committee on Appropriations and staff of that subcommittee as designated by the chair of that subcommittee, or Members of that subcommittee designated by the Chair pursuant to clause (g)(1) of Committee Rule 12.

(B) Notwithstanding the provisions of subsection (a)(1), members of the Committee and the Committee Staff may discuss and disclose only that budget-related information necessary to facilitate the enactment of the annual defense authorization bill with the chairmen and ranking minority members of the House and Senate Committees on Armed Services and the staff of those committees as designated by the chairmen of those committees.

(C) Notwithstanding the provisions of subsection (a)(1), members of the Committee and the Committee Staff may discuss with and disclose to the chair and ranking minority member of a subcommittee of the House Appropriations Committee with jurisdiction over an agency or program within the National Intelligence Program (NIP), and staff of that subcommittee as designated by the chair of that subcommittee, only that budget-related information necessary to facilitate the enactment of an appropriations bill within which is included an appropriation for an agency or program within the NIP.

(D) The Chair may, in consultation with the Ranking Minority Member, upon the written request to the Chair from the Inspector General of an element of the Intelligence Community, grant access to Committee transcripts or documents that are relevant to an investigation of an allegation of possible false testimony or other inappropriate conduct before the Committee, or that are otherwise relevant to the Inspector General's investigation.

(E) Upon the written request of the head of an Intelligence Community element, the Chair may, in consultation with the Ranking Minority Member, make available Committee briefing or hearing transcripts to that element for review by that element if a representative of that element testified, presented information to the Committee, or was present at the briefing or hearing the transcript of which is requested for review.

(F) Members and Committee Staff may discuss and disclose such matters as otherwise directed by the Committee.

(4) Records of Closed Proceedings. Any records or notes taken by any person memorializing material otherwise prohibited from disclosure by members of the Committee and Committee staff under these rules, including information received in executive session and the substance of any hearing or briefing that was closed to the public, shall remain Committee material subject to these rules and may not be publicly discussed, disclosed, or caused to be publicly discussed or disclosed, unless authorized by the Committee consistent with these rules.

(b) Non-Disclosure Agreement.

(1) Generally. All Committee Staff must, before joining the Committee Staff, agree in writing, as a condition of employment, not to divulge or cause to be divulged any classified information which comes into such person's possession while a member of the Committee Staff, to any person not a member of the Committee or the Committee Staff, except as authorized by the Committee in accordance with the Rules of the House and these Rules.

(2) Other Requirements. In the event of the termination of the Committee, members and Committee Staff must follow any determination by the House of Representatives with respect to the protection of classified information received while a member of the Committee or as Committee Staff.

(3) Requests for Testimony of Staff.

(A) All Committee Staff must, as a condition of employment, agree in writing to notify the Committee immediately of any request for testimony received while a member of the Committee Staff, or at any time thereafter, concerning any classified information received by such person while a member of the Committee Staff.

(B) Committee Staff shall not disclose, in response to any such request for testimony, any such classified information, except as authorized by the Committee in accordance with the Rules of the House and these rules.

(C) In the event of the termination of the Committee, Committee Staff will be subject to any determination made by the House of Representatives with respect to any requests for testimony involving classified information received while a member of the Committee Staff.

13. CLASSIFIED MATERIAL

(a) Receipt of Classified Information.

(1) Generally. In the case of any information that has been classified under established security procedures and submitted to the Committee by any source, the Committee shall receive such classified information as executive session material.

(2) Staff Receipt of Classified Materials. For purposes of receiving classified information, the Committee Staff is authorized to accept information on behalf of the Committee.

(b) Non-Disclosure of Classified Information. Any classified information received by the Committee, from any source, shall not be disclosed to any person not a member of the Committee or the Committee Staff, or otherwise released, except as authorized by the Committee in accordance with the Rules of the House and these rules.

(c) Exception for Non-Exclusive Materials.

(1) Non-Exclusive Materials. Any materials provided to the Committee by the executive branch, if provided in whole or in part for the purpose of review by members who are not members of the Committee, shall be received or held by the Committee on a non-exclusive basis. Classified information provided to the Committee shall be considered to have been provided on an exclusive basis unless the executive branch provides a specific, written statement to the contrary.

(2) Access for Non-Committee Members. In the case of materials received on a non-exclusive basis, the Chair, in consultation with the Ranking Minority Member, may grant non-Committee members access to such materials in accordance with the requirements of Rule 14(f)(4), notwithstanding paragraphs (1), (2), and (3) of Rule 14.

14. PROCEDURES RELATED TO HANDLING OF CLASSIFIED INFORMATION

(a) Security Measures.

(1) Strict Security. The Committee's offices shall operate under strict security procedures administered by the Director of Security and Registry of the Committee under the direct supervision of the Staff Director.

(2) U.S. Capitol Police Presence Required. At least one U.S. Capitol Police officer shall be on duty at all times outside the entrance to Committee offices to control entry of all persons to such offices.

(3) Identification Required. Before entering the Committee's offices all persons shall identify themselves to the U.S. Capitol Police officer described in paragraph (2) and to a member of the Committee or Committee Staff.

(4) Maintenance of Classified Materials. Classified documents shall be segregated and maintained in approved security storage locations.

(5) Examination of Classified Materials. Classified documents in the Committee's possession shall be examined in an appropriately secure manner.

(6) Prohibition on Removal of Classified Materials. Removal of any classified document from the Committee's offices is strictly prohibited, except as provided by these rules.

(7) Exception. Notwithstanding the prohibition set forth in paragraph (6), a classified document, or copy thereof, may be removed from the Committee's offices in furtherance of official Committee business. Appropriate security procedures shall govern the handling of any classified documents removed from the Committee's offices.

(b) Access to Classified Information by Members. All members of the Committee shall at all times have access to all classified papers and other material received by the Committee from any source.

(c) Need-to-know.

(1) Generally. Committee Staff shall have access to any classified information provided to the Committee on a strict "need-to-know" basis, as determined by the Committee, and under the Committee's direction by the Staff Director.

(2) Appropriate Clearances Required. Committee Staff must have the appropriate clearances prior to any access to compartmented information.

(d) Oath.

(1) Requirement. Before any member of the Committee, or the Committee Staff, shall have access to classified information, the following oath shall be executed:

"I do solemnly swear (or affirm) that I will not disclose or cause to be disclosed any classified information received in the course of my service on the House Permanent Select Committee on Intelligence, except when authorized to do so by the Committee or the House of Representatives."

(2) Copy. A copy of such executed oath shall be retained in the files of the Committee.

(e) Registry.

(1) Generally. The Committee shall maintain a registry that:

(A) Provides a brief description of the content of all classified documents provided to the Committee by the executive branch that remain in the possession of the Committee; and

(B) Lists by number all such documents.

(2) Designation by the Staff Director. The Staff Director shall designate a member of the Committee Staff to be responsible for the organization and daily maintenance of such registry.

(3) Availability. Such registry shall be available to all members of the Committee and Committee Staff.

(f) Requests by Members of Other Committees. Pursuant to the Rules of the House, members who are not members of the Committee may be granted access to such classified transcripts, records, data, charts, or files of the Committee, and be admitted on a non-participatory basis to classified hearings of the Committee involving discussions of classified material in the following manner:

(1) Written Notification Required. Members who desire to examine classified materials in the possession of the Committee, or to attend Committee hearings or briefings on a non-participatory basis, must notify the Chief Clerk of the Committee in writing. Such notification shall state with specificity the justification for the request and the need for access.

(2) Committee Consideration. The Committee shall consider each such request by non-Committee members at the earliest practicable opportunity. The Committee shall determine, by record vote, what action it deems appropriate in light of all of the circumstances of each request. In its determination, the Committee shall consider:

(A) The sensitivity to the national defense or the confidential conduct of the foreign relations of the United States of the information sought;

(B) The likelihood of its being directly or indirectly disclosed;

(C) The jurisdictional interest of the member making the request; and

(D) Such other concerns, constitutional or otherwise, as may affect the public interest of the United States.

(3) Committee Action. After consideration of the member's request, the Committee may take any action it deems appropriate under the circumstances, including but not limited to:

(A) Approving the request, in whole or part;

(B) Denying the request;

(C) Providing the requested information or material in a different form than that sought by the member; or

(D) Making the requested information or material available to all members of the House.

(4) Requirements for Access by Non-Committee Members. Prior to a non-Committee member being given access to classified information pursuant to this subsection, the requesting member shall:

(A) Provide the Committee a copy of the oath executed by such member pursuant to House Rule XXIII, clause 13; and

(B) Agree in writing not to divulge any classified information provided to the member, pursuant to this subsection, to any person not a member of the Committee or the Committee Staff, except as otherwise authorized by the Committee in accordance with the Rules of the House and these rules.

(5) Consultation Authorized. When considering a member's request, the Committee may consult the Director of National Intelligence and such other officials it considers necessary.

(6) Finality of Committee Decision.

(A) Should the member making such a request disagree with the Committee's determination with respect to that request, or any part thereof, that member must notify the Committee in writing of such disagreement.

(B) The Committee shall subsequently consider the matter and decide, by record vote, what further action or recommendation, if any, the Committee will take.

(g) Admission of Designated Members of the Subcommittee on Defense of the Committee on Appropriations. Notwithstanding the provisions of subsection (f), the Chair may admit no more than three designated Members of the Subcommittee on Defense of the Committee on Appropriations to classified hearings and briefings of the Committee involving discussions of classified material. Such Members may also be granted access to classified transcripts, records, data, charts or files of the Committee incident to such attendance.

(1) Designation. The Chair may designate three Members of the Subcommittee to be eligible for admission in consultation with the Ranking Minority Member, of whom not more than two may be from the same political party. Such designation shall be effective for the entire Congress.

(2) Admission. The Chair may determine whether to admit designated Members at each hearing or briefing of the Committee involving discussions of classified material. If the Chair admits any of the designated Members to a particular hearing or briefing, all three of the designated Members shall be admitted to that hearing or briefing. Designated Members shall not be counted for quorum purposes and shall not have a vote in any meeting.

(3) Requirements for Access. Prior to being given access to classified information pursuant to this subsection, a designated Member shall:

(A) Provide the Committee a copy of the oath executed by such Member pursuant to House Rule XXIII, clause 13; and

(B) Agree in writing not to divulge any classified information provided to the Member pursuant to this subsection to any person not a Member of the Committee or a designated Member or authorized Staff of the Subcommittee on Defense of the Committee on Appropriations, except as otherwise authorized by the Committee in accordance with the Rules of the House and these rules.

(h) Advising the House or Other Committees. Pursuant to Section 501 of the National Security Act of 1947 (50 U.S.C. 413), and to the Rules of the House, the Committee shall call to the attention of the House, or to any other appropriate committee of the House, those matters requiring the attention of the House, or such other committee, on the basis of the following provisions:

(1) By Request of Committee Member. At the request of any member of the Committee to call to the attention of the House, or any other committee, executive session material in the Committee's possession, the Committee shall meet at the earliest practicable opportunity to consider that request.

(2) Committee Consideration of Request. The Committee shall consider the following factors, among any others it deems appropriate:

(A) The effect of the matter in question on the national defense or the foreign relations of the United States;

(B) Whether the matter in question involves sensitive intelligence sources and methods;

(C) Whether the matter in question otherwise raises questions affecting the national interest; and

(D) Whether the matter in question affects matters within the jurisdiction of another Committee of the House.

(3) Views of Other Committees. In examining such factors, the Committee may seek the opinion of members of the Committee appointed from standing committees of the House with jurisdiction over the matter in question, or submissions from such other committees.

(4) Other Advice. The Committee may, during its deliberations on such requests, seek the advice of any executive branch official.

(i) Reasonable Opportunity to Examine Materials. Before the Committee makes any decision regarding any request for access to any classified information in its possession, or a proposal to bring any matter to the attention of the House or another committee, members of the Committee shall have a reasonable opportunity to examine all pertinent testimony, documents, or other materials in the Committee's possession that may inform their decision on the question.

(j) Notification to the House. The Committee may bring a matter to the attention of the House when, after consideration of the factors set forth in this rule, it considers the matter in question so grave that it requires the attention of all members of the House, and time is of the essence, or for any reason the Committee finds compelling.

(k) Method of Disclosure to the House.

(1) Should the Committee decide by record vote that a matter requires the attention of the House as described in subsection (i), it shall make arrangements to notify the House promptly.

(2) In such cases, the Committee shall consider whether:

(A) To request an immediate secret session of the House (with time equally divided between the Majority and the Minority); or

(B) To publicly disclose the matter in question pursuant to clause 11(g) of House Rule X.

(l) Requirement to Protect Sources and Methods. In bringing a matter to the attention of the House, or another committee, the Committee, with due regard for the protection of intelligence sources and methods, shall take all necessary steps to safeguard materials or information relating to the matter in question.

(m) Availability of Information to Other Committees. The Committee, having determined that a matter shall be brought to the attention of another committee, shall ensure that such matter, including all classified information related to that matter, is promptly made available to the chair and ranking minority member of such other committee.

(n) Provision of Materials. The Director of Security and Registry for the Committee shall provide a copy of these rules, and the applicable portions of the Rules of the House of Representatives governing the handling of classified information, along with those materials determined by the Committee to be made available to such other committee of the House or non-Committee member.

(o) Ensuring Clearances and Secure Storage. The Director of Security and Registry shall ensure that such other committee or non-Committee member receiving such classified materials may properly store classified materials in a manner consistent with all governing rules, regulations, policies, procedures, and statutes.

(p) Log. The Director of Security and Registry for the Committee shall maintain a written record identifying the particular classified document or material provided to such other committee or non-Committee member, the reasons agreed upon by the Committee for approving such transmission, and the name of the committee or non-Committee member receiving such document or material.

(q) Miscellaneous Requirements.

(1) Staff Director's Additional Authority. The Staff Director is further empowered to provide for such additional measures, which he or she deems necessary, to protect such classified information authorized by the Committee to be provided to such other committee or non-Committee member.

(2) Notice to Originating Agency. In the event that the Committee authorizes the disclosure of classified information provided to the Committee by an agency of the executive branch to a non-Committee member or to another committee, the Chair may notify the providing agency of the Committee's action prior to the transmission of such classified information.

15. LEGISLATIVE CALENDAR

- (a) Generally. The Chief Clerk, under the direction of the Staff Director, shall maintain a printed calendar that lists:
- (1) The legislative measures introduced and referred to the Committee;
 - (2) The status of such measures; and
 - (3) Such other matters that the Committee may require.
- (b) Revisions to the Calendar. The calendar shall be revised from time to time to show pertinent changes.
- (c) Availability. A copy of each such revision shall be furnished to each member, upon request.
- (d) Consultation with Appropriate Government Entities. Unless otherwise directed by the Committee, legislative measures referred to the Committee may be referred by the Chief Clerk to the appropriate department or agency of the Government for reports thereon.

16. COMMITTEE WEBSITE

The Chair shall maintain an official Committee web site for the purpose of furthering the Committee's legislative and oversight responsibilities, including communicating information about the Committee's activities to Committee members and other members of the House.

17. MOTIONS TO GO TO CONFERENCE

In accordance with clause 2(a) of House Rule XI, the Chair is authorized and directed to offer a privileged motion to go to conference under clause 1 of House Rule XXII whenever the Chair considers it appropriate.

18. COMMITTEE TRAVEL

- (a) Authority. The Chair may authorize members and Committee Staff to travel on Committee business.
- (b) Requests.
- (1) Member Requests. Members requesting authorization for such travel shall state the purpose and length of the trip, and shall submit such request directly to the Chair.
 - (2) Committee Staff Requests. Committee Staff requesting authorization for such travel shall state the purpose and length of the trip, and shall submit such request through their supervisors to the Staff Director and the Chair.
- (c) Notification to Members.
- (1) Generally. Members shall be notified of all foreign travel of Committee Staff not accompanying a member.

(2) Content. All members are to be advised, prior to the commencement of such travel, of its length, nature, and purpose.

(d) Trip Reports.

(1) Generally. A full report of all issues discussed during any travel shall be submitted to the Chief Clerk of the Committee within a reasonable period of time following the completion of such trip.

(2) Availability of Reports. Such report shall be:

(A) Available for review by any member or appropriately cleared Committee Staff; and

(B) Considered executive session material for purposes of these rules.

(e) Limitations on Travel.

(1) Generally. The Chair is not authorized to permit travel on Committee business of Committee Staff who have not satisfied the requirements of subsection (d) of this rule.

(2) Exception. The Chair may authorize Committee Staff to travel on Committee business, notwithstanding the requirements of subsections (d) and (e) of this rule,

(A) At the specific request of a member of the Committee; or

(B) In the event there are circumstances beyond the control of the Committee Staff hindering compliance with such requirements.

(f) Definitions. For purposes of this rule the term “reasonable period of time” means:

(1) No later than 60 days after returning from a foreign trip; and

(2) No later than 30 days after returning from a domestic trip.

19. DISCIPLINARY ACTIONS

(a) Generally. The Committee shall immediately consider whether disciplinary action shall be taken in the case of any member of the Committee Staff alleged to have failed to conform to any rule of the House of Representatives or to these rules.

(b) Exception. In the event the House of Representatives is:

(1) In a recess period in excess of 3 days; or

(2) Has adjourned sine die; the Chair of the full Committee, in consultation with the Ranking Minority Member, may take such immediate disciplinary actions deemed necessary.

(c) Available Actions. Such disciplinary action may include immediate dismissal from the Committee Staff.

(d) Notice to Members. All members shall be notified as soon as practicable, either by facsimile transmission or regular mail, of any disciplinary action taken by the Chair pursuant to subsection (b).

(e) Reconsideration of Chair's Actions. A majority of the members of the full Committee may vote to overturn the decision of the Chair to take disciplinary action pursuant to subsection (b).

20. BROADCASTING COMMITTEE MEETINGS

Whenever any hearing or meeting conducted by the Committee is open to the public, a majority of the Committee may permit that hearing or meeting to be covered, in whole or in part, by television broadcast, radio broadcast, and still photography, or by any of such methods of coverage, subject to the provisions and in accordance with the spirit of the purposes enumerated in the Rules of the House.

21. COMMITTEE RECORDS TRANSFERRED TO THE NATIONAL ARCHIVES

(a) Generally. The records of the Committee at the National Archives and Records Administration shall be made available for public use in accordance with the Rules of the House of Representatives.

(b) Notice of Withholding. The Chair shall notify the Ranking Minority Member of any decision, pursuant to the Rules of the House of Representatives, to withhold a record otherwise available, and the matter shall be presented to the full Committee for a determination of the question of public availability on the written request of any member of the Committee.

22. CHANGES IN RULES

(a) Generally. These rules may be modified, amended, or repealed by vote of the full Committee.

(b) Notice of Proposed Changes. A notice, in writing, of the proposed change shall be given to each member at least 48 hours prior to any meeting at which action on the proposed rule change is to be taken.

NONDISCLOSURE AGREEMENT BETWEEN HPSCI EMPLOYEES AND THE HPSCI

I, DIANE DORNAN; in consideration for being employed by or engaged by contract or otherwise to perform services for or at the request of, the House Permanent Select Committee on Intelligence (HPSCI) do hereby agree to accept as conditions precedent for my employment or engagement and for my continuing employment or engagement with the HPSCI the obligations set forth below:

1. I have read House Resolution 658 of the 95th Congress, 1st Session, which established the HPSCI. I hereby agree to be bound by the rules of the House, including those within the jurisdiction of the Committee on Standards of Official Conduct. X

2. I have also read the Rules of the HPSCI and hereby agree to be bound by them. I will never divulge, publish, or reveal by writing, word, conduct, or otherwise, either during my tenure with the HPSCI or anytime thereafter, any testimony given before the HPSCI in executive session (including the name of any witness who appeared or was called to appear before the HPSCI in executive session), the contents of any material or information received or generated by the HPSCI which has been identified under established HPSCI security procedures or Executive Order or by the Director of Central Intelligence (DCI) as requiring protection from unauthorized disclosure and to which I have access during my tenure with the HPSCI staff, or any information classified under Executive Order 11652 which may otherwise come into my possession during my tenure with the HPSCI staff, to any person not a member of the HPSCI or HPSCI staff, for any purpose or in connection with any proceeding, judicial or otherwise, except as authorized by the HPSCI in accordance with Section 7 of H. Res. 658, and the HPSCI Rules, or in the event of the termination of the HPSCI in such a manner as may be determined by the House. Nothing in this section prohibits my referencing, so long as accompanied by citation, such material or information which appears in open sources provided the use of the information does not explicitly confirm the validity of the contents of the cited material. X

3. I hereby agree to familiarize myself with the HPSCI security procedures and to provide at all times the required degree of protection for information and materials which come into my possession by virtue of my position with the HPSCI so that they will not be disclosed except as directed by the HPSCI in accordance with Section 7 of H. Res. 658 of the 95th Congress and the HPSCI Rules or in the event of the termination of the HPSCI in such a manner as may be determined by the House.

4. I hereby agree that the contents of any material or information which I am pledged not to divulge, publish or reveal by writing, word, conduct, or otherwise pursuant to Section 2 of this Agreement, and which is contemplated for publication or actually prepared for publication by me either during my tenure with the HPSCI staff or anytime thereafter,



will, prior to discussing it with or showing it to any publishers, editors, or literary agents, be submitted to the Chairman of the HPSCI who shall consult with the DCI or the DCI's designated representative, for the purpose of determining whether said material or information contains any information which I pledge hereby not to disclose. A good faith effort shall be made to arrive at such a determination and to notify me within 30 days. If the DCI and the Chairman disagree about its disclosure, I recognize that the procedures for disclosure of information described in Section 7 of H. Res. 658 of the 95th Congress shall be followed, or, in the event of the termination of the HPSCI, the procedures which may then be determined by the House. I further agree that I will not take any steps toward publication until I have received written permission from the Chairman of the HPSCI, or, in the event of the termination of the HPSCI, the authorization as may then be required by the House.

5. I hereby agree to report without delay to the HPSCI, or in the event of the termination of the HPSCI, the House, any incident where an attempt is made by any person not a member of the HPSCI staff to solicit from me information which I pledge hereby not to disclose.

6. I hereby agree to immediately notify the HPSCI, or in the event of HPSCI's termination, the House, in the event that I am called upon by the properly constituted authorities to testify or provide information which I am pledged hereby not to disclose. I will request that my obligation to testify is established before I do so.

7. I hereby agree to surrender to the HPSCI, or the DCI with the approval of the Chairman, upon demand by the Chairman of the HPSCI, or upon my separation from the HPSCI staff, all material and information which I am pledged not to divulge, publish or reveal by writing, word, conduct or otherwise pursuant to Section 2 of this agreement.

8. I understand that the HPSCI Rules provide that the employment of any staff member who violates the Rules may be immediately terminated or that other appropriate disciplinary action may be taken.

9. I understand that, in the event the HPSCI seeks to terminate my employment on the basis that I have violated the terms of this agreement, the HPSCI will provide me, in advance of my termination, a written statement setting forth the alleged violations with which I am charged.

10. I hereby assign to the United States Government all rights, title and interest in any and all royalties, remunerations, and emoluments that have resulted or will result or may result from any such divulgence, publication or revelation of information prohibited from disclosure under the terms of this agreement.

11. I understand that the United States Government may, prior to any unauthorized disclosure by me, choose to apply to any appropriate court for an appropriate order prohibiting disclosure. Nothing in this agreement constitutes a waiver on the part of the United States for criminal prosecution for any breach of this agreement on my part. Nothing in this agreement constitutes a waiver on my part of any possible defenses I may have in connection with either civil or criminal procedures which may be directed against me. Nothing in this agreement limits in any way any of the legal rights, responsibilities, or privileges which may exist for either party under H. Res. 658 or the laws or the Constitution of the United States.

12. I have read the provisions of the Espionage Laws, Sections 793, 794, and 798, Title 18 of the United States Code, and Section 783(b) of Title 50 of the United States Code and I am aware that unauthorized disclosure of certain types of information may subject me to prosecution for violation of these laws. I have read Section 1001 of Title 18, United States Code

and I am aware that the making of a false statement herein, is punishable as a felony. I have also read Executive Order ~~11652~~¹¹⁶⁵², as amended, and the implementing National Security Council Directive of 17 May 1972, as amended, relating to the protection of classified information.

13. Unless released in writing from this agreement, or any portion thereof, by the Chairman of the HPSCI with concurrence of the DCI, I recognize that all the conditions and obligations imposed on me by this agreement apply during my Committee employment or engagement and continue to apply after the relationship is terminated.

I make this agreement without any mental reservations or purpose of evasion, and I agree that it may be used by the HPSCI in carrying out its duty to protect the security of information provided to it.

Micane Moran
Signature

Apr. 22, 1985
Date

WITNESS:

[Handwritten Signature]
Signature

4-22-85
Date

Revised
05/06/99

NON-DISCLOSURE AGREEMENT
BETWEEN
HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE EMPLOYEES
AND THE
HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE

I, *Alene Roark*, in consideration for being employed by or engaged by contract or otherwise to perform services for or at the request of, the House Permanent Select Committee on Intelligence HPSCI do hereby agree to accept as conditions precedent for my employment or engagement and for my continuing employment or engagement with the HPSCI the obligations set forth below:

1. I have read House Resolution 658 of the 95th Congress, 1st Session (H.Res. 658), which established the HPSCI, I hereby agree to be bound by the Rules of the House, including those within the jurisdiction of the Committee on Standards of Official Conduct.

2. I have also read the Rules of Procedure for the HPSCI and hereby agree to be bound by them. I will never divulge, publish, or reveal by writing, word, conduct, or otherwise, either during my tenure with the HPSCI or anytime thereafter, any testimony given before the HPSCI in executive session including the name of any witness who appeared or was called to appear before the HPSCI in executive session, the contents of any material, restricted data (as that term is defined by Title 42, United States Code, Section 2014), or information received or generated by the HPSCI that has been identified under established HPSCI security procedures, by Executive Order, by the Director of Central Intelligence (DCI), or otherwise by statute, as requiring protection from unauthorized disclosure and to which I have access during my tenure with the HPSCI staff, or any information classified pursuant to any Executive Order, by the DCI, or otherwise by statute, which may otherwise come into my possession during my tenure with the HPSCI Staff, to any person not a Member of the HPSCI or HPSCI staff, for any purpose or in connection with any proceeding, judicial or otherwise, except as authorized by the HPSCI in accordance with Section 7 of H.Res. 658, and the Rules of Procedure for the HPSCI, or in the event of the termination of the HPSCI in such a manner as may be determined by the House. Nothing in this section prohibits my referencing, so long as accompanied by citation, such information, material, or restricted data that appears in open sources provides the use of the information does not explicitly confirm the validity of the contents of the cited material.



Revised
05/06/99

3. I hereby agree to familiarize myself with the HPSCI security procedures and to provide at all times the required degree of protection for the classified information, materials, and restricted data which may come into my possession by virtue of my position with the HPSCI so that such information, materials, and restricted data will not be disclosed except as directed by the HPSCI in accordance with Section 7 of H.Res. 658 and the Rules of Procedure for the HPSCI, or in the event of the termination of the HPSCI in such a manner as may be determined by the House.

4. I hereby agree that the contents of any information, material, or restricted data, which I agree not to divulge, publish, or reveal by writing, word, conduct, or otherwise, pursuant to paragraph 2 of this Agreement, and which is contemplated for publication or actually prepared for publication by me, either during my tenure with the HPSCI staff or anytime thereafter, will, prior to discussing it with, or showing it to any publishers, editors, or literary agents, be submitted to the Chairman of the HPSCI who may consult with the DCI, the DCI's designate, and other Administration officials as may be appropriate, for the purpose of determining whether such information, material, or restricted data contains anything that I hereby pledge not to disclose. A good faith effort shall be made to arrive at such a determination and to notify me within 30 days. If the DCI, the DCI Designate, or other Administration officials as may be appropriate, and the Chairman disagree about its disclosure, I recognize that the procedures for disclosure of information described in Section 7 of H.Res. 658 and the Rules of Procedure for the HPSCI shall govern, or, in the event of the termination of the HPSCI, the procedures that may then be determined by the House. I further agree that I will not take any steps toward publication until I have received written permission from the Chairman of the HPSCI, or, in the event of the termination of the HPSCI, the authorization as may then be required by the House.

5. I hereby agree to report without delay to the HPSCI, or in the event of the termination of the HPSCI to notify the House, any incident where an attempt is made by any person not a member of the HPSCI staff to solicit from me information that I hereby agree not to disclose.

6. I hereby agree to immediately notify the HPSCI, or in the event of the termination of the HPSCI to notify the House, in the event that I am called upon to testify or provide information, material, or restricted data, which I hereby agree not to disclose. I will request that my legal obligation to testify be established before I participate in such activity.

7. I hereby agree to surrender to the HPSCI, or to the DCI, the DCI's designate, or other Administration officials as may be appropriate, with the approval of the Chairman of the HPSCI, upon demand by the Chairman of the HPSCI, or upon my separation from the HPSCI staff, all information, material, or

Revised
05/06/99

restricted data, which I hereby agree not to divulge, publish, or reveal by writing, word, conduct, or otherwise, pursuant to paragraph 2 of this agreement.

8. I understand that the Rules of Procedure for the HPSCI provide that the employment of any staff member who violates such Rules may be immediately terminated or that other appropriate disciplinary action may be taken.

9. I understand that in the event the HPSCI seeks to terminate my employment on the basis that I have knowingly violated the terms of this agreement, a rule of the Committee, or any rule of the House, the HPSCI will provide me, in advance of my termination, a written statement setting forth the alleged violation.

10. I hereby assign to the United States Government all rights, title and interest in any and all royalties, remuneration, or emoluments that have resulted, or may result, from any such divulgence, publication, or revelation of information, material, or restricted data prohibited from disclosure under the terms of this agreement.

11. I understand that the United States Government may, prior to any unauthorized disclosure by me, choose to apply to any court with jurisdiction for an appropriate order prohibiting such disclosure. Nothing in this agreement constitutes a waiver on the part of the United States for civil action or criminal prosecution against me that may result from any alleged breach of this agreement resulting from my actions. Nothing in this agreement constitutes a waiver on my part of any possible defenses I may have in connection with either civil or criminal action that may be filed against me. Nothing in this agreement limits, in any way, any of the legal rights, responsibilities, or privileges that may exist for either party in either action under H.Res. 658, the Constitution, or other laws of the United States.

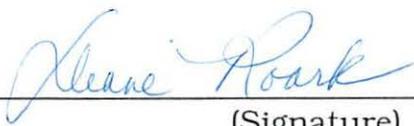
12. I am aware that Title 18, United States Code, Sections 793, 794, and 798; Title 50, United States Code, Section 783(b); and provisions within the Atomic Energy Act of 1954, proscribe the unauthorized disclosure of certain types of information, material, or restricted data. I am further aware that any unauthorized disclosure of such information, material, or restricted data may subject me to prosecution for violation of these laws. I am aware that making a false statement to any federal law enforcement officer, or to Congress (including making a false representation herein) could subject me to criminal prosecution pursuant to Title 18, United States Code, Section 1001, a felony. I have also read Executive Order 11652, as amended, and the implementing National Security Council Directive of 17 May 1972, as amended, relating to the protection of classified information.

13. Unless released in writing from this agreement, or any portion

Revised
05/06/99

thereof, by the Chairman of the HPSCI with concurrence of the DCI, the DCI's designate, and other Administration officials as may be appropriate, I recognize that all of the conditions and obligations imposed on me by this agreement apply during my Committee employment, or engagement, and continue to apply after the relationship is terminated.

I make this agreement without any mental reservations or purpose of evasion, and I agree that it may be used by the HPSCI in carrying out its duty to protect the security of information, material, or restricted data provided to it.



(Signature)

5/18/99

(Date)

WITNESS:



(Signature)

May 18, 1999

(Date)

S. AMANDA MARSHALL, OSB # 953473

United States Attorney

District of Oregon

JAMES E. COX, JR., OSB # 085653

jim.cox@usdoj.gov

Assistant United States Attorney

United States Attorney's Office

District of Oregon

1000 SW Third Ave., Suite 600

Portland, Oregon 97204-2902

Telephone: (503) 727-1026

Facsimile: (503) 727-1117

Attorneys for Defendant United States

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

DIANE ROARK,

Case No.: 6:12-CV-01354-MC

Plaintiff,

v.

**DECLARATION OF KIRSTEN M.
RUHLAND IN SUPPORT OF
DEFENDANT'S MOTION FOR
SUMMARY JUDGMENT**

UNITED STATES OF AMERICA,

Defendant.

I, Kirsten M. Ruhland, hereby make the following declaration under penalty of perjury pursuant to 28 U.S.C. § 1746. I make this declaration on personal knowledge and, if called upon to do so, I could and would competently testify to the following matters.

1. I am employed in the Security Policy Branch of the office of the Deputy Chief of Naval Operations for Information Dominance. This declaration is in support of the review I

Page 1 Declaration of Kirsten M. Ruhland in Support of Defendant's Motion for Summary Judgment

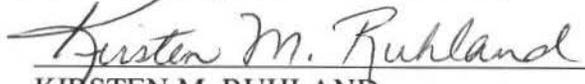
Roark v. United States, 6:12-CV-01354-MC

conducted of a document which I understand was seized from Ms. Diane Roark. The document in question is a two page correspondence dated April 28, 1999, from Commander, Naval Security Group Command to the Chief of Legislative Affairs regarding approval of an official answer from the Navy to Congress. This document and the information in the document has not been made publicly available.

2. I have consulted with the Security Director of U.S. Fleet Cyber Command/U.S. TENTH Fleet, Battlespace Awareness Program Manager for Deputy Chief of Naval Operations for Information Dominance, and reviewed OPNAVINST 5513.8B Security Classification Guide (ID#08-113). The information in the aggregate identifies a Navy program, technical organizational components, and external agency equities that require continued protection in the interest of national security. Had this document been requested through the Freedom of Information Act (FOIA), it would have been exempted from disclosure under Exemption (1)(A) of the FOIA. Section 552(b) (1)(A) of Title 5 of the U.S. Code exempts from mandatory disclosure matters “specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign policy.”

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

Executed this 30th day of September at 2014.


KIRSTEN M. RUHLAND

CERTIFICATE OF SERVICE

I hereby certify that on September 30, 2014 a copy of the foregoing **Declaration of Kirsten M. Ruhland in Support of Defendant's Motion for Summary Judgment** was placed in a postage prepaid envelope and deposited in the United States Mail at Portland, Oregon, , addressed to:

Diane Roark
2000 N. Scenic View Dr.
Stayton, OR 97383

And was sent via email to the following email address:

gardenofeden@wvi.com

/s/ James E. Cox, Jr.
JAMES E. COX, JR.

S. AMANDA MARSHALL, OSB # 953473

United States Attorney

District of Oregon

JAMES E. COX, JR., OSB # 085653

jim.cox@usdoj.gov

Assistant United States Attorney

United States Attorney's Office

District of Oregon

1000 SW Third Ave., Suite 600

Portland, Oregon 97204-2902

Telephone: (503) 727-1026

Facsimile: (503) 727-1117

Attorneys for Defendant United States

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

DIANE ROARK,

Case No.: 6:12-CV-01354-MC

Plaintiff,

v.

**DECLARATION OF CHARLES E.¹ IN
SUPPORT OF DEFENDANT'S MOTION
FOR SUMMARY JUDGMENT**

UNITED STATES OF AMERICA,

Defendant.

¹ Section 6 of the National Security Agency Act of 1959, 50 U.S.C. § 3605 (Pub. L. No. 86-36) authorizes the National Security Agency (NSA) to protect from public disclosure, among other categories of information, the names of its employees. The undersigned declarant and the NSA employee referred to in the body of this declaration occupy non-public positions with the NSA. Thus, the names of these NSA employees are referred to by first name, last initial. The Agency is prepared to provide the full name of any employee in an *ex parte*, under seal filing should the Court so require.

I, Charles E., hereby make the following declaration under penalty of perjury pursuant to 28 U.S.C. § 1746.

1. I am a Computer Forensic Examiner with the National Security Agency (NSA) and currently assigned within the Office of Counter Intelligence, Computer Forensic Investigations. I have been in this work role for approximately 2 years and have since conducted approximately 104 digital media examinations relating to security and counterintelligence issues affecting NSA and/or National Security matters. Since 2011, I have successfully completed approximately 432 training hours relevant to computer forensics, computer incident response, and network security.

2. I have been informed that the Federal Bureau of Investigation (FBI) seized a personal hard disk drive (HDD) from plaintiff Diane Roark and created a raw image copy, which was provided to me for forensic analysis. Prior to the start of analysis, I utilized the EnCase Forensic, Version 6.18.1.3, software to verify the file integrity of all images by confirming the MDS hash values were consistent with acquisition values documented by the FBI Computer Analysis and Response Team originally tasked to image the aforementioned HDD. I have completed the forensic examination of the following HDD:

Drive Model: Maxtor 6L040J2, DD Image Files Labeled: Q3_1_2.00X Serial: 662200214659
Cylinders: 77557 Heads: 16 Sectors: 63 Total Sectors: 78177792 Drive Size: 37.3 MD5 Value:
23F8BB82 5FADEC4B 455BD483 662D1077.

3. The scope of the forensic examination was to identify any data related to classified information or information protected by the National Security Agency Act of 1959 within the files located in plaintiff Roark's user profile on the HDD (the user profile is the directory "C:\Documents and Settings\Diane Roark"). Standard keyword terms associated with classified NSA and classified National Defense Information were used to search the foregoing user profile

directory, except for the jpg (picture) files and wav (audio) file. The keywords cannot be included in this declaration at an unclassified level, but include terms such as "NSA", "TOP SECRET", as well as terms specific to NSA activities. The initial keyword search was only conducted of the user profile directory and did not include any other directories, including the directories that appear to include more than 10,000 America On-Line (AOL) emails.

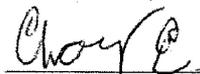
4. The initial keyword search indicated that 53 files in the user profile directory contained one or more of the keywords. I provided a copy of four of these 53 files to Miriam P., Deputy Chief of Staff for Policy and Corporate Issues for the Signals Intelligence Directorate of the NSA, for classification review.

5. Additionally, the initial keyword search did not include any search terms from the House Permanent Select Committee on Intelligence. The NSA does not have the authority to agree to the release of classified or protected information that originates from another federal agency or department. When the question of disclosure of such information arises, the NSA refers the information and the issue of disclosure to the originating agency for a decision.

6. Although there are tools and techniques designed to overwrite deleted files, various complications and/or circumstances can, and do, subvert their complete effectiveness. For example, technical issues within HDDs, such as unreadable, or "bad", sectors can prevent traditional forensic tools from accessing those areas. Also, if a user of the HDD employs any data-hiding techniques, such as encryption, locating this type of data can be difficult to discover; thus, the data would not be overwritten. I am not aware of a technical solution that completely ensures the removal of data from a HDD that does not result in the total destruction and inability to use the HDD.

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

Executed this 29th day of September 2014 at Fort Meade, Maryland.



CHARLES E.

CERTIFICATE OF SERVICE

I hereby certify that on September 30, 2014 a copy of the foregoing **Declaration of Charles E. in Support of Defendant's Motion for Summary Judgment** was placed in a postage prepaid envelope and deposited in the United States Mail at Portland, Oregon, addressed to:

Diane Roark
2000 N. Scenic View Dr.
Stayton, OR 97383

And was sent via email to the following email address:

gardenofeden@wvi.com

/s/ James E. Cox, Jr.
JAMES E. COX, JR.

S. AMANDA MARSHALL, OSB # 953473

United States Attorney

District of Oregon

JAMES E. COX, JR., OSB # 085653

jim.cox@usdoj.gov

Assistant United States Attorney

United States Attorney's Office

District of Oregon

1000 SW Third Ave., Suite 600

Portland, Oregon 97204-2902

Telephone: (503) 727-1026

Facsimile: (503) 727-1117

Attorneys for Defendant United States

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

DIANE ROARK,

Case No.: 6:12-CV-01354-MC

Plaintiff,

v.

**DECLARATION OF LAURA J. PINO IN
SUPPORT OF DEFENDANT'S MOTION
FOR SUMMARY JUDGMENT**

UNITED STATES OF AMERICA,

Defendant.

I, Laura J. Pino, hereby make the following declaration under penalty of perjury pursuant to 28 U.S.C. § 1746.

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and currently assigned to the Baltimore field office. I have been a Special Agent for approximately seventeen years. I have conducted or managed National Security investigations throughout my career.

Page 1 Declaration of Laura J. Pino in Support of Defendant's Motion for Summary Judgment

Roark v. United States, 6:12-CV-01354-MC

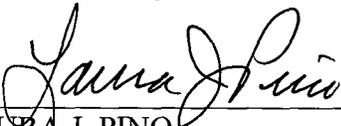
2. On or about July 26, 2007, the FBI conducted a search of plaintiff Diane Roark's residence pursuant to a search warrant. Attached hereto as Exhibit 1 is a true and correct copy of a redacted version of the affidavit submitted in support of the application for the warrant to search Roark's residence.

3. The FBI seized certain items during the search of plaintiff Roark's residence. Attached hereto as Exhibit 2 is a true and correct copy of the receipts issued to plaintiff Roark for the property seized by the FBI during the search of plaintiff Roark's residence.

4. Since the July 2007 search, the FBI has returned some of the property to plaintiff Roark that was seized. The only property that the FBI still retains from the 2007 search and seizure of plaintiff Roark's residence is the desktop computer referenced in the declaration of Charles E. and the items listed in the chart attached hereto as Exhibit 3.

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

Executed this 30th day of September 2014 at Calverton, Maryland.


LAURA J. PINO

CERTIFICATE OF SERVICE

I hereby certify that on September 30, 2014 a copy of the foregoing **Declaration of Laura J. Pino in Support of Defendant's Motion for Summary Judgment** was placed in a postage prepaid envelope and deposited in the United States Mail at Portland, Oregon, , addressed to:

Diane Roark
2000 N. Scenic View Dr.
Stayton, OR 97383

And was sent via email to the following email address:

gardenofeden@wvi.com

/s/ James E. Cox, Jr.
JAMES E. COX, JR.

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT APPLICATION

I, Christine A. Botz, being duly sworn, depose and state as follows:

I. INTRODUCTION

1. I am a Special Agent of the Federal Bureau of Investigation ("FBI") and am assigned to the Washington Field Office in the District of Columbia. I am assigned to a Counterintelligence Squad which investigates crimes involving national security. I have been an FBI Special Agent for approximately four years, have completed FBI training in the proper handling of classified information, and have been involved in the execution of search warrants and seizing evidence from residences and other locations.

2. I am currently assigned to a task force that is conducting an investigation into the unauthorized disclosure, or "leak," of classified information to two New York Times ("NYT") reporters, James Risen and Eric Lichtblau, who work in the NYT's Washington, D.C. Bureau, concerning alleged activities of the National Security Agency ("NSA"), including the Terrorist Surveillance Program ("TSP"). The investigation concerns potential violations of Title 18, United States Code (U.S.C.), Sections 793 (Unlawful Disclosure of Classified National Defense Information), 798 (Unlawful Disclosure of Classified Information) and 371 (Conspiracy To Commit an Offense Against The United States). As detailed below, the investigation to date has established probable cause to believe that William Edward Binney ("Binney"), Diane Sue Roark ("Roark"), Edward Francis Loomis ("Loomis"), and John Kirk Wiebe ("Wiebe"), have without authorization removed and retained classified documents or materials at an unauthorized location, that is, their respective homes, and disclosed such information to other persons not authorized to receive it, including at least one member of the media.

3. This affidavit is made in support of an application for warrants authorizing searches of the residences of (a) Binney, located at 7800 Elberta Drive, Severn, Maryland (described more fully in Attachment A), (b) Roark, located at 2000 North Scenic View Drive, Stayton, Oregon (described more fully in Attachment B), (c) Loomis, located at 515 Overdale Road, Baltimore, Maryland (described more fully in Attachment C), and (d) Wiebe, located at 1390 Alison Court, Westminster, Maryland (described more fully in Attachment D), and the seizure of classified information and/or evidence establishing those individuals' unauthorized removal, retention and/or disclosure of classified documents or materials, in violation of one or more of the aforementioned statutes. A listing of items to be seized at each location is described in Attachment E.

4. The facts set forth in this affidavit are those personally known to me, or communicated to me by other FBI Special Agents and personnel with knowledge of this investigation. Since this affidavit is being submitted for the limited purpose of securing search warrants, I have set forth only those facts which I believe are necessary to establish probable cause to believe that fruits, instrumentalities and/or evidence of the above-specified offenses will be located at the aforementioned premises.

II. BACKGROUND

A. The Attacks of September 11 and the Terrorist Surveillance Program

5. On September 11, 2001, the al Qaeda terrorist network launched a set of coordinated attacks along the East Coast of the United States. Four commercial jetliners, each carefully selected to be fully loaded with fuel for a transcontinental flight, were hijacked by al Qaeda operatives. Two of the jetliners were targeted at the Nation's financial center in New York and were deliberately flown into the Twin Towers of the

World Trade Center. The third was targeted at the headquarters of the Nation's Armed Forces, the Pentagon. The fourth was apparently headed toward Washington, D.C., when passengers struggled with the hijackers and the plane crashed in Shanksville, Pennsylvania. The intended target of this fourth jetliner was evidently the White House or the Capitol, strongly suggesting that its intended mission was to strike a decapitation blow on the Government of the United States – to kill the President, the Vice President or Members of Congress. The attacks of September 11 resulted in approximately 3,000 deaths, the highest single-day death toll from hostile foreign attacks in the Nation's history. The attacks shut down air travel in the United States, disrupted the Nation's financial markets and government operations, and caused billions of dollars in damage to the economy.

6. On September 14, 2001, the President declared a national emergency “by reason of the terrorist attacks at the World Trade Center, New York, New York, and the Pentagon, and the continuing and immediate threat of further attacks on the United States.” Proclamation No. 7463, 66 Fed. Reg. 48,199 (Sept. 14, 2001). The same day, Congress passed a joint resolution authorizing the President “to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks” of September 11, which the President signed on September 18. Authorization for Use of Military Force, Pub. L. No. 107-40, § 2(a), 115 Stat. 224, 224 (Sept. 18, 2001) (reported as a note to 50 U.S.C.A. § 1541). Congress also expressly acknowledged that the attacks rendered it “necessary and appropriate” for the United States to exercise its right “to protect United States citizens both at home and abroad,” and in particular recognized that “the President has authority

under the Constitution to take action to deter and prevent acts of international terrorism against the United States.” *Id.* pmbl. Congress emphasized that the attacks “continue to pose an unusual and extraordinary threat to the national security and foreign policy of the United States.” *Id.* The United States also launched a large-scale military response, both at home and abroad. In the United States, combat air patrols were immediately established over major metropolitan areas and were maintained 24 hours a day until April 2002. The United States also immediately began plans for a military response directed at al Qaeda’s base of operations in Afghanistan. Acting under his constitutional authority as Commander in Chief, and with the support of Congress, the President dispatched forces to Afghanistan and, with the assistance of the Northern Alliance, toppled the Taliban regime.

7. Against this unfolding background of events in the fall of 2001, there was substantial concern that al Qaeda and its allies were preparing to carry out another attack within the United States. Al Qaeda had demonstrated its ability to introduce agents into the United States undetected and to perpetrate devastating attacks, and it was suspected that additional agents were likely already in position within the Nation’s borders. To counter this threat, the President authorized the NSA to intercept international communications into and out of the United States of persons linked to al Qaeda or related terrorist organizations. Press Conference of President Bush (Dec. 19, 2005), *available at* <http://www.whitehouse.gov/news/releases/2005/12/20051219-2.html>. This activity – which subsequently was identified as the Terrorist Surveillance Program (TSP) – was “critical” to national security and was designed to establish an early warning system to detect and prevent another catastrophic terrorist attack on the United States. Press

Briefing by Attorney General Alberto Gonzales and General Michael Hayden (Dec. 19, 2005), available at <http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html>.

B. The Unauthorized Disclosure Of Classified Information Concerning The TSP

8. In early October 2004, James Risen contacted Public Affairs officials in the Office of the Vice President, the National Security Council, the Central Intelligence Agency ("CIA") and the NSA about a news article he was writing. The Public Affairs officials and other high-ranking Executive Branch officials have confirmed that during the ensuing days, Risen engaged in a series of email communications, conversations and meetings with the officials regarding the story. In substance, Risen represented that he had obtained information about a warrantless electronic surveillance program that he said was known to only a few officials within the United States Government. Ultimately, Risen's inquiries led to a meeting on October 25, 2004, at The White House, involving other representatives of The New York Times and high-ranking Executive Branch officials. This was followed by another meeting about ten days later at the Department of Justice involving Risen, Lichtblau, a third NYT representative, and several high-ranking Executive Branch officials. Subsequent to this meeting, NYT representatives elected not to publish Risen's story without first conferring further with the high-ranking Executive Branch officials. As a result, no story regarding the TSP was published in 2004.

9. Approximately one year later, in the fall of 2005, NYT representatives again contacted high-ranking Executive Branch officials and advised that they were considering publishing the story. In that regard, it was represented that additional "sources" had come forward and raised concerns about the surveillance activities. A number of meetings ensued between representatives of The New York Times, high-ranking

Executive Branch officials and Members of Congress. Despite these ongoing discussions, NYT published its story on its website the evening of December 15, 2005. The story, titled *Bush Lets U.S. Spy on Callers Without Courts*, was authored by Risen and Lichtblau and appeared in the next day's edition of the newspaper. This article was followed by a series of NYT articles, written or co-authored by Risen and/or Lichtblau describing a range of alleged NSA activities and related circumstances, including:

a. *Spy Agency Mined Vast Data Trove, Officials Report*, Dec. 24, 2005, by James Risen and Eric Lichtblau;

b. *Defense Lawyers in Terror Cases Plan Challenges Over Spy Efforts*, Dec. 28, 2005, by James Risen and Eric Lichtblau;

c. *Justice Deputy Resisted Parts of Spy Program*, Jan. 1, 2006, by James Risen and Eric Lichtblau; and

d. *Spy Agency Data After Sept. 11 Led FBI to Dead Ends*, Jan. 17, 2006, by Lowell Bergman, Eric Lichtblau, Scott Shane and Don Van Natta, Jr.

10. In early January 2006, Risen published a book, titled State of War: The Secret History of the CIA and the Bush Administration. Chapter 2 of the book was entitled, "The Program," and dealt entirely with alleged NSA activities, including the warrantless surveillance program described in the Risen and Lichtblau articles.

11. Since publication of the aforementioned articles and book, there have been numerous additional stories in various media, including but not limited to newspapers, magazines, television, radio and the internet, regarding the TSP and related matters. As set forth below, one such article, which appeared in 2006,

titled

by

suggests that one or more of the four subjects discussed herein disclosed highly classified information concerning the NSA and its activities, sources and methods, to unauthorized persons.

III. INVESTIGATION OF THE LEAK OF CLASSIFIED INFORMATION CONCERNING THE TSP

12. Shortly after the first TSP article, in late December 2005, the DOJ and the FBI initiated an investigation concerning the unauthorized disclosure of classified information contained in that article. That investigation has been continuing since that time and has involved interviews of in excess of 1,000 individuals, issuance of more than 200 grand jury subpoenas, principally for telephone and email records, and review of thousands of pages of documents, including telephone and email records for approximately 60 individuals.

A. Background Regarding Four Subjects Of The Investigation

13. Through that process, the following individuals, among others, have been identified as subjects of the investigation: (a) William Binney, a former senior operations officer for the NSA, who now resides in Severn, Maryland; (b) Diane Roark, a former staff member on the U.S. House of Representatives Permanent Select Committee on Intelligence (HPSCI), who now resides in Stayton, Oregon; (c) Edward Loomis, a former cryptologic computer scientist at NSA, who now resides in Baltimore, Maryland; and (d) John Wiebe, a former acting division chief at NSA, who now resides in Westminster, Maryland.

14. Binney is a former senior operations officer for the NSA who retired on October 31, 2001, after 36 years of service. Since 2004, Binney has worked as a contractor for the NSA and has entered NSA facilities approximately two times a year.

After retiring, Binney started a three-person contracting firm on December 3, 2001, with Loomis and Wiebe. The company is called Entity Mapping LLC (Entity). According to Binney, the company has done work for NSA, Boeing, and the Department of Homeland Security. In addition to being a partner in Entity, Binney worked for Eagle Alliance from October 2001 to October 2002; Zytel Corporation (General Dynamics sub-contractor) from November 22, 2002, to May 5, 2004; Diversified Development Corporation from July 2002 to the present; and Entegra Systems, Inc. from October 2005 to the present. While working at the NSA, Binney was the program manager of a program called "THIN THREAD." Additionally, he had regular contact with Roark while she was serving as a HPSCI staff member. At no time during or subsequent to his employment at the NSA has Binney been authorized to possess NSA classified documents or data at his home or on his personal computer.

15. Roark is a former Congressional staff member who worked for seventeen years on the HPSCI until she retired in April 2002. At the HPSCI, Roark assisted in oversight of various compartmentalized intelligence programs at the NSA, as well as related Congressional budget approval issues. After Roark left the HPSCI, she stayed in the Washington, D.C., area until early 2003, when she moved to Oregon. At no time during or subsequent to her service on the HPSCI has Roark been authorized to possess NSA classified documents or data at her home or on her personal computer.

16. Loomis is a former cryptologic computer scientist for the NSA who retired in November 2001 after twelve years of service. Since the end of 2002, Loomis has worked as a contractor for the NSA and has entered NSA facilities on a regular basis. After retiring, Loomis started Entity, the above mentioned three-person contracting firm, with

Binney and Wiebe. The company's corporate headquarters is located at 515 Overdale Road, Baltimore, Maryland, which is also Loomis's home address. In addition to being a partner in Entity, Loomis worked for Eagle Alliance from November 2001 to October 2002; GTE Tactical Systems (General Dynamics sub-contractor) from November 2002 to present; and Diversified Development Corporation from October 2002 to the present. At no time during or subsequent to his employment at the NSA has Loomis been authorized to possess NSA classified documents or data at his home or on his personal computer.

17. Wiebe is a former acting division chief for the NSA who retired in October 2001 after approximately 26 years of service. After Wiebe retired from the NSA, he continued to work as a contractor for the NSA and regularly has entered NSA facilities. On December 3, 2001, Wiebe started Entity with Binney and Loomis. In addition to being a partner in Entity, Wiebe worked for Eagle Alliance from October 2001 to November 2002; Diversified Development Corporation from September 2002 to the present; and GTE Tactical Systems (General Dynamics sub-contractor) from April 2003 to present. At no time during or subsequent to his employment at the NSA has Wiebe been authorized to possess NSA classified documents or data at his home or on his personal computer.

B. The Subjects' Unlawful Disclosure Of Classified NSA Information

1. Roark And Binney To Disclose The To Unauthorized Persons

18. According to NSA officials who have been interviewed in connection with this investigation, in the mid to late 1990s, Binney, Loomis and Wiebe worked on several programs that _____ at the NSA. One of these _____ programs,

which Binney claimed during an FBI interview that he developed,¹ was called

According to Binney, was a pre-cursor to the
Moreover, Binney believed that was less costly than the and
included purportedly designed to address
associated with NSA activities.

19. Both before and after 9/11, Binney, as the project manager,
provided Roark, as the HPSCI staff member with NSA responsibilities, with information
regarding According to Binney, Roark was a strong proponent of the
program and worked hard to ensure that it was funded. However,
according to Binney and several other NSA employees who were interviewed during this
investigation, Roark did not have an accurate understanding of and
believed it was

20. Binney explained to the FBI that after 9/11, the NSA decided to scale back
the program. By his own admission, Binney was extremely upset about
this decision. Moreover, at or about the same time, Binney learned that the was
being implemented. Significantly, Binney admitted that he was never "read in" to the
TSP program – that is, he was never authorized to receive information concerning the
program. He also has admitted, however, that he learned of its existence, its covername
(which remains unpublished today) and its basic outlines, from an NSA contractor who
was not authorized to provide Binney this classified information.

¹ Binney has been interviewed by the FBI on three occasions during this investigation: October 19, 2006, March 21, 2007, and June 28, 2007. The statements attributed to Binney in this affidavit were made during one or more of those interviews.

21. Binney advised the FBI that because he was upset at NSA's decision to scale back _____ in favor of the _____ he went to Roark, his contact on the HPSCI. According to Binney, in late 2001, while Roark was still with the HPSCI, Binney met her at her home in Hyattsville, Maryland, and told her what he knew about the TSP. According to NSA officials, Roark also had not been read in to the TSP (indeed, she has never been read in). Nevertheless, Binney informed the FBI that he and Roark then discussed various actions they could take to bring their concerns about the TSP to the attention of people within and outside the United States Government.

22. According to Binney, one step that he and Roark took was to disclose the existence of the TSP to Dale Griffiths, another NSA contractor who, according to NSA officials, was not read in to the TSP. According to Binney, Griffiths was a friend of the daughter of a U.S. Supreme Court Justice, and Binney and Roark hoped that Griffiths could facilitate a meeting with the Justice through the daughter. Binney told the FBI that this effort failed. Binney further stated that at or about the same time, Roark told him that she had called the presiding judge of the Foreign Intelligence Surveillance Court (FISC), Judge Colleen Kollar-Kotelly, to arrange a meeting; however, after an exchange of telephone calls with a court secretary, Roark was told to convey any concerns she had to the DOJ.

23. According to Binney, in late 2001 or early 2002, Roark arranged for him and Wiebe to brief a member of the HPSCI about the TSP. According to NSA officials, that member was not read in to the TSP. Roark also told Binney that she went to the Chairman of the HPSCI, _____ to discuss the TSP. According to the Chairman, who has been interviewed during the investigation, he told Roark to speak

with General Michael Hayden, then the Director of the NSA, regarding her concerns. According to Binney, Roark told him that she spoke with General Hayden regarding her concerns about the TSP, as well as her belief that _____ was a superior program. Roark subsequently told Binney that as far as she was aware, no action was taken by the NSA after her discussion with General Hayden.

2. **Binney, Roark, Loomis And Wiebe Disclose Classified NSA Information Without Authorization**

24. During his interview(s) with the FBI, Binney stated that in 2002, after he had left the NSA, he, Roark, Loomis and Wiebe created a thirteen-page summary of the _____ technology on his home computer. The idea to create the document originated with Roark, who wrote the first draft. Binney, Wiebe, and Loomis subsequently wrote technical parts of the summary which the four subjects then e-mailed back and forth to one another from their home computers. The subjects wrote the document as part of their effort to market innovative information technology solutions to potential customers, including government agencies, in connection with their fledgling contracting business.

25. According to Binney, when the final document was completed in May 2002, Binney and Loomis, who are not NSA classification authorities, and were not even NSA employees at the time, conducted their own "classification review" and decided that the document was unclassified. Notably, Binney stated that no effort was made by Roark, Binney, Loomis, or Wiebe to submit the _____ summary for classification review by appropriate authorities at the NSA. Binney told the FBI that they based their classification decision on the fact that there was "far worse" on the internet as other contractor firms were far more open with their information than was the

memorandum and, if it was acceptable for other firms to be open about their classified or sensitive information, it was acceptable for them.

26. In connection with this and other investigations in which I have participated, I have learned that individuals who hold security clearances typically sign agreements that they will safeguard classified information, report violations of security rules, and not disseminate classified information to uncleared persons. This matter is no exception. On November 22, 2002, Binney signed a security agreement with the NSA governing his obligations regarding "protected information," which is defined in the agreement as "information obtained as a result of my relationship with NSA which is classified or in the process of a classification determination." Wiebe signed the same agreement on October 24, 2002, and Loomis signed it on November 21, 2002. The security agreement, a copy of which has been obtained in connection with the investigation, states, in pertinent part:

I understand that all Protected Information to which I may obtain access hereafter, is and will remain the property of the United States Government unless and until otherwise determined by an appropriate official or final ruling of a court of law.... I agree not to discuss matters pertaining to Protected Information except when necessary for the proper performance of my duties and only with persons who are currently authorized to receive such information and have a need-to-know...I understand the burden is upon me to determine whether information or materials within my control are considered by the NSA to be protected information, and whether the person(s) to whom disclosure is to be made is/are authorized to receive it.

In the agreement, Binney, Wiebe and Loomis also acknowledged that the unauthorized disclosure of "protected information" may constitute a violation of one or more of the following statutes – Sections 793, 794, 798, or 952 of Title 18, United States Code, and

sections 421 through 426 and 783(b) of Title 50, United States Code.

27. The security agreement also contained a provision regarding the return of “protected information,” underscoring its contraband nature if it is maintained in an uncleared space such as a person’s home:

I do not now, nor will I ever, possess any right, interest, title, or claim whatsoever to such information. I agree that upon demand by an authorized representative of the NSA or upon the conclusion of my authorized access to Protected Information, I shall return all material concerning such Protected Information in my possession, or for which I am responsible because of such access. I understand that failure to return such items may be a violation of Section 793 of Title 18, United States Code, and may constitute a crime for which I may be prosecuted.

28. Although Roark did not sign a security agreement with the NSA, she had signed one with the _____ which was similar in substance to the NSA agreement, as recently as July 24, 2001. A copy of that signed agreement also has been obtained and reviewed in connection with this investigation. In addition to the foregoing, I know from interviews of numerous Congressional officials that Roark, as a HPSCI staff member, regularly received and conducted briefings about highly classified programs and regularly was advised of the requirements and limitations associated with access to classified information. Indeed, in connection with this and other “leak” investigations in which I have participated, numerous Congressional officials have been interviewed, including elected officials and staff members, and all have acknowledged a knowledge and understanding of their responsibilities and duties with regard to classified information. This includes an obligation not to disclose classified information to unauthorized persons. Roark’s knowledge of these requirements is further evidenced by the fact that about eight months after the TSP “leak,” she submitted a proposed editorial

to the [redacted] for pre-publication review. Since the editorial addressed SIGINT equities, the [redacted] deferred the classification ruling to NSA. In the editorial, a copy of which has been obtained and reviewed in connection with this investigation, Roark touted the advantages of [redacted] over the [redacted]. According to NSA officials, Roark eventually was notified that the article she had submitted was not approved for publication because it contained classified information.

3. **The Unauthorized Disclosure Of Classified NSA Information To A Member Of The Media**

29. Notwithstanding the foregoing, on [redacted] 2006, an article was published in [redacted] titled [redacted] by [redacted] which championed [redacted] over the [redacted]. During an interview of a former high-ranking FBI official in connection with this investigation, that official stated that before publication of the [redacted] 2006 story, [redacted] contacted her and asked for information about the [redacted] specifically identifying it by the initials of the covername for [redacted]. Although the [redacted] article itself did not contain classified information, the questions [redacted] asked the FBI official and the information set forth below strongly suggest that [redacted] source or sources for [redacted] story related classified [redacted] information to [redacted].

30. In that regard, Binney explained to the FBI that shortly before publication of the [redacted] 2006 article, Roark called Binney from her home in Oregon and told him she was talking to [redacted] and that [redacted] was working on an article about [redacted]. According to Binney, Roark further explained that the article was going to highlight [redacted] was cheaper than the [redacted] and had [redacted].

that the [redacted] did not have – issues that Roark previously had raised with HPSCI members and General Hayden. Roark also asked Binney if he would talk to [redacted] but he declined.

31. Binney has further advised the FBI that during the same conversation, Roark asked him if the [redacted] he had done on the [redacted] program occurred in [redacted] and Binney confirmed that it had. Roark concluded the conversation by asking Binney to e-mail her the thirteen-page summary of [redacted] that she, Binney, Loomis and Wiebe had written in 2002 and which contained details about the architecture of [redacted]

According to Binney, he still had the document on his computer and e-mailed it from Binney3@verizon.net, his personal email address on his home computer, to dr20781@aol.com, Roark's personal email address on her home computer, with a copy to Wiebe at jkwiebe@comcast.net, his personal email address on his home computer.

32. When asked about the [redacted] 2006 article by the FBI, Binney admitted that his answer to Roark's question about [redacted] in [redacted] appeared in the article. Likewise, he admitted that the article's discussion of [redacted]

[redacted] seems to be directly lifted from the thirteen-page summary he provided to Roark. I believe that this suggests, at a minimum, that Roark read portions of the summary to [redacted] Moreover, she may have provided the entire document by hand, fax or email. According to Binney, before he sent the [redacted]

summary to Roark, she asked if he and Loomis would review the document to confirm it was unclassified. Binney then confirmed that he and Loomis believed it was unclassified. While this facially suggests that Roark was sensitive to classification issues, it is worth noting that she, Binney and Loomis were no longer employed by the federal [redacted]

government, were not classification authorities, were fully aware of the appropriate procedure for seeking classification determinations, and never sought review of the document by the NSA before transmitting it through unsecure channels and sharing it with an uncleared member of the media.

33. During his June 28, 2007 FBI interview, less than thirty days ago, Binney was asked if he still had the e-mail he sent to Roark in May 2006. Binney claimed that he no longer had the e-mail due to a computer virus. According to Binney, in the summer or fall of 2006, Binney and Wiebe had to “wipe” Binney’s personal computer because it was infected with a virus. It should be noted, however, that Binney was first interviewed by the FBI about _____ related matters on October 19, 2006, at or around the time he wiped his computer. In spite of this fact, Binney admitted that as of June 28, 2007, he still had a copy of the thirteen-page _____ summary on his computer, claiming he was able to “reconfigure” the document.

34. During the June 28, 2007 interview, Binney also indicated that he was told by Roark that she was “called in” to see the FBI, and that Binney should be careful and see an attorney as his name was brought up during her FBI meeting. Binney originally said Roark e-mailed this information to him; however, when he was asked for the e-mail by the interviewing agent, Binney changed his story and said that Roark had visited him and sent him a letter with the information. When asked for the letter, Binney said that he threw it away.

C. NSA’s Review Of The Thirteen-Page

Summary

35. On March 25, 2007, several days after his second FBI interview, Binney voluntarily e-mailed to the FBI the thirteen-page _____ summary which he

originally had helped create in 2002. On May 10, 2007, the FBI provided that document to the NSA and requested that it conduct a thorough classification review of the summary. On June 26, 2007, NSA officials advised the FBI that the summary is a classified document at the _____ level. As described above, this document was created, edited and emailed by and between Binney, Roark, Loomis and Wiebe. Moreover, there is reason to believe that Roark may have transmitted it to _____ at or about the time _____ article was published. Thus, it appears that a _____ document, classified drafts of the document, and/or classified information contained in or relating to the document, _____ were and are located on the personal computers and in the residences of Binney, Roark, Loomis and Wiebe.

IV. PREMISES TO BE SEARCHED AND ITEMS TO BE SEIZED

36. The investigation has established that 7800 Elberta Drive, Severn, Maryland, is Binney's primary residence. The property is a two-story, single family home in a subdivision, and is further described in Attachment A. The property also contains a light colored storage shed, which is located in the backyard, to the west of the residence, near several large trees. A property ownership search conducted through a Lexis-Nexis, a public database, on July 9, 2007, indicates that "William E. Binney" is the owner and occupant of the residence. "Carole J. Binney" is also listed as an owner and occupant. Binney is married to Carole J. Binney. "Matthew C. Binney" and "David A. Binney" are also occupants. Both Matthew and David are sons of Binney. On June 27, 2007, FBI Special Agents visited the premises to be searched and observed a maroon Ford Crown Victoria parked at the above address. This vehicle is registered to William

Binney.

37. Binney was interviewed at this location on June 28, 2007. During this interview, Binney went to a room on the second floor to print off e-mail addresses for Roark, Wiebe, and Loomis, from his home computer. During this same interview, Binney gave the interviewing agent a business card that showed he was a Partner in Entity Mapping, LLC, which listed a business address of 7800 Elberta Road, Severn, Maryland, his residence. Thus, it appears that Binney works from his home, and uses it as his office, Binney also maintains personal and business records in his home and, given his technical expertise, will most likely maintain documents and information in various electronic storage devices and media there.

38. The investigation has further established that 2000 N. Scenic View Drive, Stayton, Oregon, is Roark's primary residence. The property is a one-story, single family home, with a finished attic and basement, located in a cul-de-sac, and is further described in Attachment B. A property ownership search conducted through Lexis-Nexis, a public database, on July 16, 2007, indicates that "Diane S. Roark" is the sole owner and occupant of the residence. According to the Marion County Assessor's report, the property is owned by Diane S. Roark and also contains a storage shed or "machine shed" of approximately 384 square feet in size. Oregon DMV records reflect that Diane S. Roark's drivers license lists her address as 2000 N Scenic View Drive, Stayton, Oregon and she has one vehicle registered in her name at that address.

39. The investigation has further established that 515 Overdale Road, Baltimore, Maryland, is Loomis's primary residence. The property is a two-story, single family home with a basement, and is further described in Attachment C. A property

ownership search conducted through Lexis-Nexis, a public database, on July 9, 2007, indicates that "Edward F. Loomis Jr." is the owner and occupant of the residence. "Kathlene D. Loomis" is also listed as an owner and occupant. Loomis is married to Kathlene D. Loomis.

40. The investigation has further established that 1390 Alison Court, Westminster, Maryland, is Wiebe's primary residence. The property is a two-story, single family home, and is further described in Attachment D. A property ownership search conducted through Lexis-Nexis, a public database, on July 9, 2007, indicates that "John K. Wiebe" is the owner and occupant of the residence. "Cynthia L. Wiebe" is also listed as an owner and occupant. Wiebe is married to Cynthia L. Wiebe. "Kristen M. Wiebe" is also an occupant. Kristen is a daughter of Wiebe.

41. As noted above, Binney, Roark, Loomis and Wiebe conduct business out of their respective homes. Given that fact, and based upon my experience, I believe there is probable cause to believe that those individuals currently maintain in the premises to be searched documents such as calendars, datebooks, day planners, rolodexes, address books, phone logs, phone number lists, message slips, and/or other lists reflecting business associates and other contacts, including their phone numbers, addresses, email addresses, and other identifying and contact information. In that regard, they would need to be able to access such contact/address information for "ready-reference," in order to be able to make and return phone calls or otherwise maintain contact with current or former business and professional contacts. Such records serve as an information source or basis for ongoing or future contacts. In this particular case, for example, a rolodex, dayplanner, datebook, address book, and other similar types of documents referenced in

Attachment E will be particularly probative because they may provide evidence of contacts, communications, appointments, and/or meetings by and between the subjects, members of the media and others.

42. Additionally, I believe there is probable cause to believe that the subjects would also maintain in the premises to be searched the modern-electronic day business tools which one uses to maintain contact with business associates and others and keep appointments: a personal computer, a laptop or notebook computer, facsimile machine, a personal digital assistant, an electronic organizer, an electronic calendar, or a similar device. Moreover, with respect to email accounts, Binney advised the FBI that he and the other subjects of this affidavit maintain personal computers and send and receive email. He specifically identified the following email addresses associated with and used by the individual noted after the address: binney3@verizon.net (Binney); dr20781@aol.com (Roark); jkwiebc@comcast.net (Wiebe); eloomis@erols.com (Loomis); bill@entitymapping.com (Binney); ed@entitymapping.com (Loomis); kirk@entitymapping.com (Wiebe); and all@entitymapping.com (jointly used by Binney, Loomis and Wiebe). Based on my experience, I believe there is probable cause to believe that email address books on the subjects' personal computers will likely contain email addresses and or other identifying information for the business associates and other contacts with whom they have maintained, or continue to maintain, email communication. My experience with most email programs and email address books also suggests that in many instances, even if an individual writes to another individual on only one occasion, the email address listed in the "to" portion of the email message will be automatically registered into the sender's email address book. Even if the sender never

again sends a message to that individual, the sender's email address book will likely continue to preserve the recipient's email address for a future occasion when the sender contemplates emailing a message to that address.

43. Based on my experience, I also believe there is probable cause to believe that the subjects may currently possess other materials in the premises to be searched and on their personal computers, such as files, newspaper clippings, newspaper articles, books or other reading material, photographs, email messages, or other documents and material regarding _____ or related matters, as well as evidence of conversations, meetings, and/or other contact about these subjects. Accordingly, I request authorization to seize and search all such computers and related devices, as described in Attachment E, in order to obtain information and evidence that is within the scope of the requested search.

44. Based on my experience, I also know that individuals who use cellular telephones, cordless telephones, and hard line telephones often enter the other party's phone number into the memory or address book on their telephone, provided those telephones have a memory and/or phone book feature. Moreover, depending on how recently a call was made or received, the telephone itself may contain a listing of calls made to and from that phone. Accordingly, in connection with the requested searches, I also seek permission to seize such telephones for further analysis, as these items, too, may yield evidence of telephone contact by and between the subjects and others connected to the events described in this affidavit.

45. Additionally, as noted above, both Binney and Roark appear to have storage sheds located on their respective properties. Since both Binney and Roark appear

to work from home, both Binney and Roark may retain files, documents, and other personal and business records in their respective storage sheds. In my experience, individuals use garages, attics, and such storage sheds as annexes in which files, documents, and other records may be stored for reference. Accordingly, the storage sheds located on Binney's and Roark's respective properties are specified in Attachments A and B as part of the premises to be searched.

V. SEARCH PROCEDURES FOR SEARCH OF COMPUTER DATA

46. Based upon my training, experience, and information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including hard disk drives, floppy drives, compact disks, magnetic tapes, memory chips, and the like. I also know that searching computerized information for evidence or instrumentalities of a crime commonly requires agents to seize most or all of a computer system's input/output peripheral devices, related software documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. This is true for the following reasons:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer

hardware and storage devices may contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted; and

c. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography, a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband, or instrumentalities of a crime.

47. In searching for data capable of being read, stored, or interpreted by a computer, law enforcement personnel executing this search warrant will employ some or all of the following procedures:

a. Law enforcement personnel trained in searching and seizing

computer data (the "computer personnel") will assist with the search of the computers and other electronic media referenced herein to determine whether these items contain any evidence and instrumentalities of violations of federal law. The computers and other electronic media referenced herein will be reviewed by appropriately trained personnel and the case investigators in order to extract and seize any relevant data; and

b. The analysis of electronically stored data may entail any or all of several different techniques. Such techniques may include, but shall not be limited to, surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); "opening" or reading the first few "pages" of such files in order to determine their precise contents; "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic "key-word" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

48. In searching the data, the computer personnel and case investigators may examine all of the data contained in the computers and other electronic media referenced herein to view their precise contents and determine whether the data is relevant to the investigation. In addition, the computer personnel may search for and attempt to recover "deleted," "hidden," or encrypted data to determine whether the data is relevant to the investigation.

49. Although the thirteen-page summary initially was created by the subjects in 2002, the information set forth above establishes that Binney has retained it

through at least March 2007, and emailed to Roark in May 2006. Because the document and related materials were created for a business purpose, and Binney, Loomis and Wiebe are still engaged in that business activity, I believe there is probable cause to believe that the documents have been retained by all of the subjects and will be found at the search locations, including on their respective computers. Even if the electronic documents have been "deleted," however, it is my understanding that they can be recovered through technologies available to those who conduct such searches.

50. Based on my knowledge, training, and experience, including the experience of other agents with whom I have spoken, I am aware that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space - for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only

overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

51. Based upon my training and experience, I believe that the original computer and data storage media constitute evidence and should be retained by my agency. The original is necessary to address questions that may be raised about the authenticity of any document or other data extracted from the storage devices. If the items are not within the ambit of Attachment E, the government will return these items within a reasonable period of time not to exceed 60 days from the date of seizure unless further authorization is obtained from the Court.

VI. OTHER SPECIAL PROCEDURES FOR THE ROARK SEARCH

52. Roark has retained counsel in this matter, and documents that may be seized from Roark's residence may reflect confidential, attorney-client privileged communications. Therefore, I am cognizant of the possible application of the attorney-client privilege to some of the documents. Consequently, special procedures will be undertaken to ensure that no attorney-client privileged materials are provided to any member of the prosecution team, including FBI agents or DOJ prosecutors working on this investigation. The following procedures will be used:

a. No agent connected with this investigation will actually conduct any part of the review of any documents during the search. Agents participating in the search will be briefed so that they will recognize potentially privileged material. During the search, all potentially privileged material will be marked and segregated from other

documents;

b. Following the seizure of the materials, a complete inventory will be left on site and the documents seized will be available for review (subject to appropriate security clearances) for a one-week period prior to release to the prosecution team for any assertion of privilege; and

c. A review attorney from DOJ not connected with the investigation will review all seized documents to determine whether a privilege attaches. Items potentially subject to a claim of privilege will remain segregated. Upon a determination that an item is not privileged, that item will be returned to its place with other seized materials. A log will be maintained detailing the disposition of each document in question. Items which are found to be subject to a privilege will be returned to Roark. If items are found to be subject to privilege, but it is also found that an exception to the privilege applies, such as the crime-fraud exception, that item will be submitted to the court for a privilege determination. Finally, if there is any question as to whether a document is privileged, that document will be submitted to the court for a privilege determination.

VII. CONCLUSION

53. Based upon the evidence set forth herein, which I believe to be truthful and reliable, as well as my investigative experience, I believe that probable cause exists to believe that William Binney, Diane Roark, Edward Loomis and John Wiebe have engaged in the unauthorized disclosure of classified documents or materials to one another and other persons not authorized to receive it, including at least one member of the media, in violation of Title 18, United States Code, Sections 793 (Unlawful

Disclosure of Classified National Defense Information), 798 (Unlawful Disclosure of Classified Information), and 371 (Conspiracy To Commit An Offense Against The United States). I further submit that a search of the above-described premises and containers therein will result in the seizure of items listed in Attachment E that may constitute the evidence, instrumentalities, or fruits of these offenses.

SA Christine A. Botz
Christine A. Botz, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on this 25 day of July, 2007

John J. J. J.
United States Magistrate Judge
District of Oregon

Attachment A

Property to be Searched

The residence of William Binncy, located at 7800 Elberta Drive, Severn, Maryland, more particularly described as follows:

7800 Elberta Drive, Severn, Maryland, is a two-story single family residence in a residential neighborhood, located on the west side of Elberta Drive, just north of Elberta Court. Elberta Drive ends in a cul-de-sac, and the search location is on the cul-de-sac. The residence has white or cream vinyl siding. An attached two car garage is located on the left side of the residence. The street facing windows are all bracketed by blue window shutters, the roof is a light colored composite tile, and the front door is a dark color. The residence sits on property which is approximately 19,383 square feet in size. The property also contains a light colored storage shed, which is located in the backyard, to the west of the residence, near several large trees. The shed is light colored and appears to be prefabricated.

Attachment B

Property to be Searched

The residence of Diane Roark, located at 2000 N. Scenic View Drive, Stayton, Oregon, more particularly described as follows:

2000 N. Scenic View Drive, Stayton, Oregon is a one-story, single family home, with a finished attic and basement. The residence has a dark brown roof and the building is light brown or tan in color. The residence is located at the north end of a cul-de-sac. There is a red sign on the left side of the driveway with the address 2000 North Scenic View Drive on it. The residence has a circular driveway and an attached garage. The residence has a green front door with gold lamps on either side of the door. The front door faces to the south. The property also contains a dark brown wooden shed, which lies to the right side of driveway.

Attachment C

Property to be Searched

The residence of Edward Loomis, located at 515 Overdale Road, Baltimore, Maryland, more particularly described as follows:

515 Overdale Road, Baltimore, Maryland, is a two-story, single family home with a basement, located in a rural neighborhood. The residence is located on the east side of Overdale Road where it intersects with Woodside Road. The residence is a combination of red brick on the first two floors, and white vinyl siding covering the peak of the roof. A detached two car garage is located to the right of the residence. The garage is a combination of red brick on the corners and white vinyl siding covering the peak of the garage above the garage door. The garage door is white with four glass windows. The street facing windows are all bracketed by black window shutters, the roof is a gray colored shale tile, and the front door is a white color and set up four steps from the front walkway.

Attachment D

Property to be Searched

The residence of John Wiebe, located at 1390 Alison Court, Westminster, Maryland, more particularly described as follows:

1390 Alison Court, Westminster, Maryland, is a two-story, single family home in a rural neighborhood. The residence has light gray colored siding. An attached three car garage is located on the first floor of the residence. The garage has three separate garage doors. The house is located on the west side of Alison Court just south of Warehime Road. Alison Court ends in a cul-de-sac, but the residence is located at the end of a long private driveway before the cul-de-sac. The long private driveway twists to the right, past one home on the left, then one home on the right and terminates in the garage of the residence. The residence is obscured by large trees in front of the home.

Attachment E

Items to be Seized

Any items which constitute evidence, instrumentalities, or fruits of violation of Title 18, United States Code, Sections 371 (Conspiracy To Commit An Offense Against The United States), 793 (Unlawful Disclosure of Classified National Defense Information), and 798 (Unlawful Disclosure of Classified Information), including specifically:

1. U.S. government documents, classified documents (including classified documents missing headers and footers), national defense intelligence documents and papers, and other documents relating to the National Security Agency (NSA).
2. Papers or documents relating to the transmittal of U.S. government documents, national defense and classified intelligence to representatives of the news media, or individuals not authorized to receive the information;
3. Computer hardware, meaning any and all computer equipment, including any electronic devices that are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. Included within the definition of computer hardware is any data processing hardware (such as central processing units and self-contained laptop or notebook computers); internal and peripheral storage devices (such as floppy disks, compact disks/CD-roms, hard disk drives, flash drives, tapes, or similar data storage devices/media); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); related communications devices (such as modems, cables and connections); and any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as "dongles," keycards, physical keys, and locks).
4. Computer software, meaning any and all information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems software, applications software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.
5. Computer-related documentation, meaning, any written, recorded, printed, or electronically-stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.
6. Computer passwords and data security devices, meaning any devices, programs, or data – whether themselves in the nature of hardware or software – that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any

computer hardware, computer software, computer-related documentation, or electronic data records. Such items include, but are not limited to, data security hardware (such as encryption devices, chips, and circuit boards); passwords; data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data or to otherwise render programs or data into usable forms.

7. Any computer or electronic records, documents, and materials, including those used to facilitate interstate communications, in whatever form and by whatever means such records, documents, or materials, their drafts or their modifications, may have been created or stored, including, but not limited to, any hand-made form (such as writing or marking with any implement on any surface, directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures or photocopies); any mechanical form (such as photographic records, printing, or typing); and electrical, electronic, optical, or magnetic form (such as data storage devices, tape recordings, cassettes, compact disks/CD-roms, optical disks, or the like), as well as printouts and readouts from any such storage devices.
8. Any electronic information or data, stored in any form, which has been used or prepared for use either for periodic or random backup (whether deliberate, inadvertent, or automatically or manually initiated), of any computer or computer system. The form such information might take includes, but is not limited to, floppy disks fixed, hard disks, removable hard disk cartridges, tapes, laser disks, compact disks/CD-roms, video cassettes, and other media capable of data storage.
9. Any electronic storage device capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and using electronic data, in the form of electronic records, documentation, and materials, including those used to facilitate interstate communications. Included within this paragraph is any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer-related equipment, such as floppy disk drives and disks, fixed hard disks, removable hard disk cartridges, tape drives and tapes, optical storage devices, laser disks, or other data storage devices.
10. Any personal digital assistants or electronic organizers, electronic calendars, or similar devices.
11. Any facsimile machines.
12. Any mobile/cellular telephone, cordless telephone, and land-line telephone with a memory and/or phone book feature.
13. Any and all phone records, to include, but not limited to, land-line phone records and cellular phone records.

14. Any and all notebooks, sheets of papers, or writing pads, including, but not limited to, those with typed or handwritten notes which relate to the _____ program, the Terrorist Surveillance Program or other classified U.S. Government programs.
15. Any and all calendars, datebooks, day planners, rolodexes, address books, notes, journals, phone logs, phone number lists, message slips, other lists, electronic or otherwise, reflecting business associates and other contacts of personal associates, including their phone numbers, addresses, email addresses, dates of meetings or appointments, and other identifying and contact information; and/or other written correspondence that constitutes a record of telephonic contact, meetings, or appointments.
16. Any files, newspaper clippings, newspaper articles, books or other reading material, photographs, correspondence, email messages, or other documents and material, whether in hardcopy or electronic format, which concern the program or the Terrorist Surveillance Program, including, but not limited to, documents or records describing, commenting, highlighting or annotating *New York Times* articles about the Terrorist Surveillance Program, the book State of War: The Secret History of the CIA and the Bush Administration, or _____ articles.
17. Any correspondence, emails, documents, calendar or diary entries, electronic files, contact information, or data of any kind which reflect or relate to any communications or contacts of any kind with _____ or any other reporter, journalist, employee or representative of _____

FD-597 (Rev 8-11-94)

Page 1 of 1

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property Received/Returned/Released/Seized

File # 332A-HQ-1516536

On (date) 7-26-07

item(s) listed below were:

- Received From
- Returned To
- Released To
- Seized

(Name) Diane Roark

(Street Address) 2000 N. Scenic View Dr

(City) Stoughton OR

Description of Item(s):

C3) Dell Dimension 6200 CPU, service tag J9m4011

Received By: [Signature]
(Signature)

Received From: [Signature]
(Signature)

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property Received/Returned/Released/Seized

File # 332A-HQ-1516536

On (date) 7-26-07

- item(s) listed below were:
- Received From
 - Returned To
 - Released To
 - Seized

(Name) Diane Roark

(Street Address) 2000 N Scenic View Drive

(City) Stoughton

Description of Item(s):

- 1) one email dated 3/30/00
- 2) AT+T phone records, Wil. may Co statements, handwritten notes
- 3) Nokia cell phone, ESN (w/charger) 067034380257325541, 803-2776
- 4) rolodex
- 5) Emails + documents re CCDC and Graybeard
- 6) H.R 4301 report, Sp AF personnel notes
- 7) 2 classified documents
- 8) 2 folders NSA related docs, personnel papers, FOUO docs + CD "Star Sapphire Working Group 4/19/01"
- 9) CRS controlled items, 1 FOUO doc, binder "Laws Affecting the NSA"
- 10) Thin Thread folders/docs
- 11) TSP/Thin Thread documents folders
- 12) Rolodex
- 13) one box containing calendars, day planners, notebooks, bus. cards
- 14) Emails, articles + cal. adtres
- 15) Brother MFCT420 fax machine, SN U61278H5J613846
- 16) Attorney docs (not entered into AES) cy
- 17) 11 books from office - NSA subject matter

Received By: [Signature]
(Signature)

Received From: [Signature]
(Signature)

FD-597 (Rev 8-11-94)

Page 2 of 2

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property Received/Returned/Released/Seized

File # 332A HQ-1516536

On (date) 7-26-07

item(s) listed below were:

- Received From
- Returned To
- Released To
- Seized

(Name) Dane Roark

(Street Address) 2000 N. Seaside View Dr

(City) Stayton, OR

Description of Item(s):

18) Notebook "2007 work lists"

19) emails, USIC related docs, notebook

20) phone numbers, contact info

Received By: [Signature]
(Signature)

Received From: [Signature]
(Signature)

Paper documents, CD, and Notebooks Containing Classified/Protected information - 30 Sept. 2014

Number	Description/ File name	Protected Information Holder	# pages
HC1	Email strings: Re: suggestions tonight?	NSA, HPSCI	9
HC2	Congressional Staff Visit, dated 24 June 1999	NSA, HPSCI	2
HC3	Memorandum for Commander, Naval Security Group Command	NSA, HPSCI, Naval Ops for Info Dominance	2
HC4	Commander Naval Security Group Slides	NSA, HPSCI	18
HC5	Set of miscellaneous documents, primarily faxes	NSA, HPSCI	38
HC6	Intelligence Review: Audit report	HPSCI	23
HC7	Working Group April 19, 2001 CD	NSA, HPSCI	13 sample pages printed from CD for review.
HC8	CIA Responses to the Honorable Curt Weldon's Questions	RETURN	11
HC9	Intelligence Community Information Systems Strategic Plan	HPSCI	68 pages in addition to covers
HC10	Handwritten Notes: Why We're Different	RETURN	4 pages, notes on 6 sides
HC11	Pre-publication review submission	NSA, HPSCI	4
HC12	Pre-publication review submission	NSA, HPSCI	4
HC13	Pre-publication review submission	NSA, HPSCI	4
HC14	Initial Comments Regarding Specific Redactions 9/11/06	NSA, HPSCI	5
HC15	Testimony of May 18, 2006	RETURN	2
HC16	Email Excerpts: Not supposed to make sense ...	HPSCI	1
HC17	Email Excerpt: Anybody see or read ...	RETURN	4 (Copied onto 3 pages for NSA review)
HC18	Email Excerpt: They are using ...	RETURN	2 (Copied onto 1 page for NSA review)
HC19	Email Excerpt: What ethics?	HPSCI	1
HC20	Email Excerpt: ... the SSCI and HPSCI authorization language ...	HPSCI	1
HC21	Baseline (definition) Slide	HPSCI	1
HC22	NIPF Issues Agenda	RETURN	1
HC23	Notebook: At a Glance 2000	NSA	90
HC24	Notebook: 6/96- Message Log (audio)	NSA	55

UNCLASSIFIED

HC25	Notebook: tel. msg. 7/98 – 2/23/99	NSA	71
HC26	Notebook: Telephone Msg 2/24/99 to 7/21/99	NSA	68
HC27	Notebook: msg 9/28/99 to 4/6/00	NSA	63
HC28	Notebook: msg 4/6/00 to 12/1/00	NSA	69
HC29	Notebook: 12/4/00 -	NSA	67
HC30	Notebook: Week At a Glance Appointments 1998	RETURN	74
HC31	Notebook: Telecons 10/97 – 6/98	NSA	69
HC32	Notebook: (Black) Pocket Planner (Inside: 1990 calendar)	NSA	103
HC33	Notebook: (Black) Week At a Glance (Inside: Appointments 1999)	NSA	101
HC34	Notebook: 1995 – 96 Msg log (audio)	NSA	38
HC35	Notebook: Press List Telecons 4/23/97 to 9/25/97	NSA	42
HC36	Notebook: msg 7/22 – 9/27/99	NSA	51
HC37	Notebook: 2001 Desk Master Diary	RETURN	No page count shown
HC38	Email Excerpt (shorter excerpt than HC 19): What ethics?	RETURN	1

UNCLASSIFIED

FILED 10 OCT '14 11:57 USDC-ORE

Diane Roark, pro se
2000 N. Scenic View Dr.
Stayton, Oregon 97383
(503) 767-2490

UNITED STATES DISTRICT COURT
DISTRICT OF OREGON

DIANE ROARK

Case No. : 6:12-CV-01354-MC

Plaintiff,

v.

**UNOPPOSED MOTION FOR EXTENSION
OF TIME TO FILE REPLY TO
DEFENDANT'S MOTION FOR
SUMMARY JUDGMENT AND
MEMORANDUM IN SUPPORT**

UNITED STATES OF AMERICA,

Defendant

Diane Roark, pro se, submits this unopposed motion for extension of time to reply to Defendant's motion. Pursuant to Local Rule 7-1, the undersigned has conferred with Defendant regarding this motion, and Defendant does not oppose the motion.

The current deadline for filing a reply is October 24, 2014. Plaintiff requests a 33-day extension, to November 26, 2014.

This case seeks return of property under Federal Rule of Criminal Procedure 41(g). It involves issues related not only to criminal law but also to national security classification standards, claims of a unique National Security Agency right to withhold "protected" but unclassified material, legislative privilege, and other complications.

Plaintiff previously agreed in a telephone conference call on August 4, 2014, to a response time of three weeks, mistakenly thinking that this applied only to the legislative privilege issue. Because all aspects of the case are being considered simultaneously, the currently scheduled 24 days will be insufficient time to reply to the government's multiple arguments.

Plaintiff is pro se. Research, writing and formatting require much longer than for licensed government or private attorneys. Many government attorneys apparently also contributed to or reviewed the government's motion and supporting memorandum, including some with specialties in national security and legislative law. In addition to Assistant United States Attorney James Cox, these include at minimum one or more attorneys each from: the Federal Bureau of Investigation; the National Security Agency; the House Permanent Select Committee on Intelligence (HPSCI); and the Office of General Counsel of the U.S. House of Representatives.

The government received 57 days to prepare its motion and supporting memorandum (August 4 to September 30, 2014). Plaintiff requests equal time, i.e. another 33 days beyond the 24 now allotted.

Plaintiff earlier sought an expedited schedule for considering a legislative search issue in order to facilitate the long-delayed recovery of professional materials by Thomas Drake in a related Maryland Rule 41(g) case. However, this is no longer relevant because HPSCI, facilitated by NSA, proceeded with its own search of Mr. Drake's materials prior

to Court consideration of legislative privilege in Plaintiff's related instant case, and is now finalizing return of documents that it does not dispute.

Plaintiff also needs an extension because she has been able to conduct only minimal research while the government was preparing its motion and had no time to address the case during the first week after receiving the motion. Plaintiff made a previous undated commitment involving travel, and ultimately this was required in late September. A previous commitment involving about a week of volunteer work also arose and had to be fulfilled before mid-September.

Obligations unrelated to legal research will continue through the proposed extension. A contracted roof replacement in September required unexpected removal, repair and painting of some house siding, and adjacent siding still must be painted from atop the now-completed roof. Occupants of an apartment owned by Plaintiff decided unexpectedly to move abroad in mid-September; considerable refurbishment, now partially accomplished, is needed so it can be rented again. Autumn also brings many days of work on Plaintiff's three acres of landscape.

For the foregoing reasons, Plaintiff respectfully requests that the Court extend the time for filing a reply to the government's motion for summary judgment by 33 days, from October 24 to November 26.

DATED this 9th day of October 2014.

Respectfully submitted,

Diane Roark, pro se

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing **Unopposed Motion for Extension of Time To File Response to Defendant's Motion for Summary Judgment** was placed in a postage prepaid envelope and deposited in the United States Mail at Stayton, Oregon on October 9, 2014, addressed to:

James E. Cox, Jr., AUSA
United States Attorney's Office
District of Oregon
1000 SW Third Ave., Suite 600
Portland, Oregon 97204-2902

And via email to:

jim.cox@usdoj.gov

DIANE ROARK
Pro se