

1 Linda Lye (CA SBN 215584)
2 llye@aclunc.org
3 Matthew T. Cagle (CA SBN 286101)
4 mcagle@aclunc.org
5 AMERICAN CIVIL LIBERTIES UNION
6 FOUNDATION OF NORTHERN CALIFORNIA, INC.
7 39 Drumm Street
8 San Francisco, CA 94111
9 Tel: (415) 621-2493
10 Fax: (415) 255-8437

11 Patrick Toomey (admitted *pro hac vice*)
12 ptoomey@aclu.org
13 Anna Diakun (admitted *pro hac vice*)
14 adiakun@aclu.org
15 AMERICAN CIVIL LIBERTIES UNION
16 FOUNDATION
17 125 Broad Street, 18th Floor
18 New York, NY 10004
19 Tel: (212) 549-2500
20 Fax: (212) 549-2654

21 Attorneys for Plaintiffs

22 UNITED STATES DISTRICT COURT
23 FOR THE NORTHERN DISTRICT OF CALIFORNIA
24 SAN FRANCISCO-OAKLAND DIVISION

25 AMERICAN CIVIL LIBERTIES UNION
26 OF NORTHERN CALIFORNIA;
27 AMERICAN CIVIL LIBERTIES UNION;
28 AMERICAN CIVIL LIBERTIES UNION
FOUNDATION,

Plaintiffs,

v.

DEPARTMENT OF JUSTICE,

Defendant.

Case No. 4:17-cv-03571 JSW

DECLARATION OF ANNA DIAKUN IN
SUPPORT OF PLAINTIFFS' OPPOSITION
TO DEFENDANT'S MOTION AND CROSS-
MOTION FOR SUMMARY JUDGMENT

Hearing Date: November 17, 2017
Time: 9:00 a.m.
Location: Oakland U.S. Courthouse
Judge: Hon. Jeffrey S. White

1 **I, ANNA DIAKUN, PURSUANT TO 28 U.S.C. § 1746, DECLARE AS FOLLOWS:**

2 1. My name is Anna Diakun. I am counsel for Plaintiffs in the above-referenced
3 action. The information in this declaration is based upon my personal knowledge and if called
4 upon to testify, I could and would competently testify thereto.

5 2. I submit this declaration in support of Plaintiffs' Opposition to Defendant's
6 Motion for Summary Judgment and Cross-Motion for Summary Judgment. Plaintiffs are the
7 American Civil Liberties Union of Northern California, the American Civil Liberties Union, and
8 the American Civil Liberties Union Foundation (together, the "ACLU").

9 3. I am an attorney with the National Security Project at the ACLU. In my capacity
10 as an attorney, I work on issues pertaining to, among other things, privacy, technology, and
11 electronic surveillance.

12 4. On February 6, 2017, Plaintiffs sent a Freedom of Information Act ("FOIA")
13 request to Defendant Department of Justice ("DOJ") seeking records related to the government's
14 official policy on the use of evidence obtained through secret surveillance and its duty to notify
15 individuals whose private communications the government has seized and searched. Plaintiffs
16 sought expedited processing of the request because the government's policies concerning when it
17 must disclose surveillance implicate the privacy interests of numerous Americans, who are often
18 unable to challenge the lawfulness of government searches without proper notice. This request is
19 particularly urgent because Section 702 of FISA, under which many of these searches are
20 conducted, is currently the subject of intense legislative and public debate. *See* 28 C.F.R.
21 §16.5(d)(1)(iv) (setting forth standards for granting expedited processing of FOIA requests). A
22 true and correct copy of the FOIA request is attached as Exhibit 1 to this declaration.

23 5. By email dated February 10, 2017, DOJ, via its component National Security
24 Division ("NSD"), acknowledged receipt of the Request and assigned it reference number 17-
25 064. DOJ informed Plaintiffs that it had conducted a search and had located two responsive
26 records. The first record it identified was two-page cover memorandum, which DOJ withheld in
27 full pursuant to Exemption 5, specifically the deliberative process privilege and the attorney
28 work-product privilege, as well as Exemptions 6 and 7(c). The second record it identified was a

1 memorandum titled “Determining Whether Evidence is ‘Derived From’ Surveillance Under Title
2 III or FISA.” DOJ withheld this record in full pursuant to Exemption 5, specifically the
3 deliberative process privilege and the attorney work-product privilege. DOJ did not invoke the
4 attorney-client privilege as to either of these documents. A true and correct copy of NSD’s
5 February 10, 2017 email is attached as Exhibit 2 to this declaration.

6 6. On February 22, 2017, Plaintiffs timely filed an administrative appeal from DOJ’s
7 decision. Plaintiffs challenged the adequacy of DOJ’s search, its improper withholding of the
8 records under Exemptions 5, 6, and 7(C), and its failure to segregate all non-exempt information
9 in the records. A true and correct copy of Plaintiffs’ February 22, 2017 administrative appeal is
10 attached as Exhibit 3. On February 22, 2017, DOJ’s Office of Information Policy (“OIP”)
11 acknowledged receipt of the appeal, assigning it tracking number DOJ-AP-2017-002487.

12 7. On March 17, 2017, Sean R. O’Neill, Chief of the Administrative Appeals Staff at
13 OIP, responded to the appeal, affirming on partly modified grounds. Mr. O’Neill stated that DOJ
14 “properly withheld this information in full because it is protected from disclosure under the
15 FOIA pursuant to” Exemptions 5, 6, and 7(c). Mr. O’Neill further stated that the documents were
16 withholdable under Exemption 5 because they were protected by the attorney work-product
17 privilege, but not the deliberative process privilege, as DOJ had previously asserted. A true and
18 correct copy of DOJ’s March 17, 2017 letter is attached as Exhibit 4.

19 8. Plaintiffs filed this action on June 21, 2017. *See* ECF No. 1.

20 9. Attached hereto as Exhibit 5 is a true and correct copy of Office of the Director of
21 National Intelligence, 2016 Statistical Transparency Report (Apr. 2017),
22 https://www.dni.gov/files/icotr/ic_transparency_report_cy2016_5_2_17.pdf.

23 10. Attached hereto as Exhibit 6 is a true and correct copy of Admin. Office of the
24 U.S. Courts, Wiretap Report 2016, [http://www.uscourts.gov/statistics-reports/wiretap-report-](http://www.uscourts.gov/statistics-reports/wiretap-report-2016)
25 2016.

26 11. Attached hereto as Exhibit 7 is a true and correct copy of Barton Gellman, Julie
27 Tate & Ashkan Soltani, *In NSA-Intercepted Data, Those Not Targeted Far Outnumber the*
28 *Foreigners Who Are*, Wash. Post, July 5, 2014, <http://wapo.st/1mVEPXG>.

1 12. Attached hereto as Exhibit 8 is a true and correct copy of Zack Whittaker, *With a*
2 *Single Wiretap Order, US Authorities Listened in on 3.3 Million Phone Calls*, ZDNet, June 30,
3 2017, <http://www.zdnet.com/article/one-federal-wiretap-order-recorded-millions-phone-calls>.

4 13. Attached hereto as Exhibit 9 is a true and correct copy of DOJ, Revised FISA Use
5 Policy as Approved by the Attorney General (Jan. 10, 2008), <https://perma.cc/3WV2-9WZQ>.

6 14. Attached hereto as Exhibit 10 is a true and correct copy of Hearing Before the
7 Subcommittee on Crime, Terrorism, and Homeland Security on H.R. 3179, 108th Cong. 14
8 (2004) (statement of Daniel Bryant, Asst. Att’y Gen., Office of Legal Policy),
9 http://commdocs.house.gov/committees/judiciary/hju93715.000/hju93715_of.htm.

10 15. Attached hereto as Exhibit 11 is a true and correct copy of Charlie Savage,
11 *Debate Brews Over Disclosing Warrantless Spying*, N.Y. Times, Sept. 30, 2014,
12 [https://www.nytimes.com/2014/10/01/us/debate-simmers-over-disclosing-warrantless-](https://www.nytimes.com/2014/10/01/us/debate-simmers-over-disclosing-warrantless-spying.html)
13 [spyng.html](https://www.nytimes.com/2014/10/01/us/debate-simmers-over-disclosing-warrantless-spying.html).

14 16. Attached hereto as Exhibit 12 is a true and correct copy of 154 Cong. Rec. S335
15 (daily ed. Jan. 25, 2008) (statement of Sen. Kyl).

16 17. Attached hereto as Exhibit 13 is a true and correct copy of DOJ Office of Legal
17 Counsel, Applicability of FISA’s Notification Provision to Security Clearance Adjudications
18 (June 3, 2011), <https://fas.org/irp/agency/doj/olc/fisa-clear.pdf>.

19 18. Attached hereto as Exhibit 14 is a true and correct copy of Adam Liptak, *A Secret*
20 *Surveillance Program Proves Challengeable in Theory Only*, N.Y. Times, July 15, 2013,
21 <https://nyti.ms/2yxfh14>.

22 19. Attached hereto as Exhibit 15 is a true and correct copy of the relevant pages of
23 Br. for Pets., *Clapper v. Amnesty Int’l USA*, 568 U.S. 398 (2013) (No. 11-1025), 2012 WL
24 3090949.

25 20. Attached hereto as Exhibit 16 is a true and correct copy of the relevant pages of
26 Tr. of Oral Argument, *Clapper v. Amnesty Int’l USA*, 568 U.S. 398 (2013) (No. 11-1025),
27 https://www.supremecourt.gov/oral_arguments/argument_transcripts/2012/11-1025.pdf.

1 21. Attached hereto as Exhibit 17 is a true and correct copy of Charlie Savage, *Door*
2 *May Open for Challenge to Secret Wiretaps*, N.Y. Times, Oct. 16, 2013,
3 <https://nyti.ms/2tZDU3H>.

4 22. Attached hereto as Exhibit 18 is a true and correct copy of Charlie Savage,
5 *Federal Prosecutors, in a Policy Shift, Cite Warrantless Wiretaps as Evidence*, N.Y. Times, Oct.
6 26, 2013, <https://nyti.ms/2n9gb1p>.

7 23. Attached hereto as Exhibit 19 is a true and correct copy of Mem. in Opp. to Mot.
8 to Compel Discovery, *Hasbajrami v. United States*, No. 1:13-cv-06852-JG (E.D.N.Y. Aug. 8,
9 2014), ECF No. 79.

10 24. Attached hereto as Exhibit 20 is a true and correct copy of Sari Horwitz, *Justice Is*
11 *Reviewing Criminal Cases that Used Surveillance Evidence Gathered under FISA*, Wash. Post,
12 Nov. 15, 2013, <http://wapo.st/177ZZi1>.

13 25. Attached hereto as Exhibit 21 is a true and correct copy of the Hearing to
14 Consider the Nominations of John P. Carlin & Francis X. Taylor, 113th Cong. 25 (2014)
15 (statement of John P. Carlin), [https://www.intelligence.senate.gov/sites/default/files/hearings/](https://www.intelligence.senate.gov/sites/default/files/hearings/CHRG-113shrg93212.pdf)
16 [CHRG-113shrg93212.pdf](https://www.intelligence.senate.gov/sites/default/files/hearings/CHRG-113shrg93212.pdf).

17 26. Attached hereto as Exhibit 22 is a true and correct copy of *Organization, Mission*
18 *and Functions Manual: National Security Division*, DOJ <http://bit.ly/2fWYrlc>.

19 27. Attached hereto as Exhibit 23 is a true and correct copy of *Organization, Mission*
20 *and Functions Manual: Criminal Division*, DOJ, <http://bit.ly/2wpgmXO>.

21 28. Attached hereto as Exhibit 24 is a true and correct copy of DOJ, Memorandum re:
22 Department Charging and Sentencing Policy (May 10, 2017), [https://www.justice.gov/opa/press-](https://www.justice.gov/opa/press-release/file/965896/download)
23 [release/file/965896/download](https://www.justice.gov/opa/press-release/file/965896/download).

24 29. Attached hereto as Exhibit 25 is a true and correct copy of DOJ, Guidance
25 Regarding § 851 Enhancements in Plea Negotiations (Sept. 24, 2014), [https://www.justice.gov/](https://www.justice.gov/oip/foia-library/ag_guidance_on_section_851_enhancements_in_plea_negotiations/download)
26 [oip/foia-library/ag_guidance_on_section_851_enhancements_in_plea_negotiations/download](https://www.justice.gov/oip/foia-library/ag_guidance_on_section_851_enhancements_in_plea_negotiations/download).

LOCAL RULE 5-1(i)(3) CERTIFICATION

I, Linda Lye, hereby attest in accordance with Local Rule 5-1(i)(3) that the signatory to this document has concurred in its filing.

Dated: September 29, 2017

/s/ Linda Lye

Linda Lye

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Exhibit 1

LEGAL DEPARTMENT



February 6, 2017

FOIA/PA Mail Referral Unit
Justice Management Division
Department of Justice
Room 115
LOC Building
Washington, DC 20530-0001
E-mail: MRUFOIA.Requests@usdoj.gov

Arnetta Mallory
FOIA Initiatives Coordinator
National Security Division
Department of Justice
Room 6150
950 Pennsylvania Avenue, N.W.
Washington, DC 20530-0001
E-mail: nsdfoia@usdoj.gov

Chief, FOIA/PA Unit
Criminal Division
Department of Justice
Suite 1127, Keeney Building
Washington, DC 20530-0001
Email: crm.foia@usdoj.gov

FOIA/Privacy Staff
Executive Office for United States Attorneys
Department of Justice
Room 7300, 6000 E Street, NW
Washington, DC 20530-0001
Email: USAEO.FOIA.Requests@usdoj.gov

Laurie Day, Chief, Initial Request Staff
Office of Information Policy, Office of the Attorney General, and
Office of the Deputy Attorney General
Department of Justice
Suite 11050
1425 New York Avenue, N.W.
Washington, DC 20530-0001

**AMERICAN CIVIL LIBERTIES
UNION FOUNDATION**
NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500
WWW.ACLU.ORG

OFFICERS AND DIRECTORS
SUSAN N. HERMAN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

ROBERT B. REMAR
TREASURER

Re: Request Under Freedom of Information Act / Expedited Processing Requested

To Whom It May Concern:

This letter constitutes a request (“Request”) pursuant to the Freedom of Information Act (“FOIA”), 5 U.S.C. § 552 *et seq.*, and its implementing regulations.¹ The Request is submitted by the American Civil Liberties Union, the American Civil Liberties Union Foundation, and the American Civil Liberties Union of Northern California (collectively “ACLU”).²

The ACLU seeks disclosure of Department of Justice documents concerning a core Fourth Amendment question bearing on the privacy rights of Americans: in what circumstances does the Department of Justice consider information or evidence to be “derived from” surreptitious surveillance, including surveillance conducted under the Foreign Intelligence Surveillance Act (“FISA”) and the Wiretap Act (“Title III”). The Department’s answer to this question affects when it notifies Americans that their phone calls, emails, and other internet communications have been seized and searched by the government. Without such notice, Americans typically have no way of discovering that they have been surveilled, and thus no way of seeking court review of these searches and seizures of their private communications.

Public release of this information is urgently needed. The government conducts thousands of wiretaps and other searches under FISA and Title III each year. The government’s notice policies therefore implicate the privacy interests of numerous Americans, who are generally unable to challenge the lawfulness of government searches without proper notice. Moreover, official disclosures show that the Department of Justice for years failed to notify criminal defendants when evidence was “derived from” surveillance under Section 702 of FISA. As part of the ongoing debate about whether to reauthorize Section 702 when it expires this year, Congress is presently considering whether reforms to Section 702 are necessary. Information about how the government is interpreting key

¹ See 28 C.F.R. § 16.1.

² The American Civil Liberties Union Foundation is a 26 U.S.C. § 501(c)(3) organization that provides legal representation free of charge to individuals and organizations in civil rights and civil liberties cases, and educates the public about the civil liberties implications of pending and proposed state and federal legislation, provides analyses of pending and proposed legislation, directly lobbies legislators, and mobilizes its members to lobby their legislators. The American Civil Liberties Union is a separate non-profit, 26 U.S.C. § 501(c)(4) membership organization that educates the public about the civil liberties implications of pending and proposed state and federal legislation, provides analysis of pending and proposed legislation, directly lobbies legislators, and mobilizes its members to lobby their legislators.

elements of FISA is critical to this public debate and these imminent legislative judgments.

* * *

I. Records Requested

1. The memorandum titled “Determining Whether Evidence Is ‘Derived From’ Surveillance Under Title III or FISA,”³ as well as:
 - a. Any cover letter or other document attached to this memorandum;
 - b. Any version of this memorandum created or distributed on or after November 23, 2016, whether considered “final” or otherwise; and
 - c. Any record modifying, supplementing, superseding, or rescinding this memorandum or its contents.

* * *

We request that responsive electronic records be provided electronically in their native file format. *See* 5 U.S.C. § 552(a)(3)(B). Alternatively, we request that the records be provided electronically in a text-searchable, static-image format (PDF), in the best image quality in the agency’s possession, and in separate, Bates-stamped files.

II. Request for Expedited Processing

We request expedited processing pursuant to 5 U.S.C. § 552(a)(6)(E) and the statute’s implementing regulations. There is a “compelling need” for these records, as defined in the statute and regulations, because the information requested is urgently needed by an organization primarily engaged in disseminating information in order to inform the public about actual or alleged government activity. 5 U.S.C. § 552(a)(6)(E)(v); *see also* 28 C.F.R. § 16.5(e)(1)(ii); 28 C.F.R. § 16.5(e)(1)(iv).

A. The ACLU is an organization primarily engaged in disseminating information in order to inform the public about actual or alleged government activity.

The ACLU is “primarily engaged in disseminating information” within the meaning of the statute and relevant regulations. 5 U.S.C. § 552(a)(6)(E)(v)(II); 28 C.F.R. § 16.5(e)(1)(ii). *See ACLU v. Dep’t of Justice*, 321 F. Supp. 2d 24, 30 n.5 (D.D.C. 2004) (finding that a non-profit, public-interest group that “gathers information of potential interest to a segment of the

³ The ACLU understands that a final version of this document was distributed within the Department of Justice on November 23, 2016.

public, uses its editorial skills to turn the raw material into a distinct work, and distributes that work to an audience” is “primarily engaged in disseminating information” (internal citation omitted)); *see also Leadership Conference on Civil Rights v. Gonzales*, 404 F. Supp. 2d 246, 260 (D.D.C. 2005) (finding Leadership Conference—whose mission is to “disseminate[] information regarding civil rights and voting rights to educate the public [and] promote effective civil rights laws”—to be “primarily engaged in the dissemination of information”).

Dissemination of information about actual or alleged government activity is a critical and substantial component of the ACLU’s mission and work. The ACLU disseminates this information to educate the public and promote the protection of civil liberties. The ACLU’s regular means of disseminating and editorializing information obtained through FOIA requests include: a paper newsletter distributed to approximately 450,000 people; a bi-weekly electronic newsletter distributed to approximately 300,000 subscribers; published reports, books, pamphlets, and fact sheets; a widely read blog; heavily visited websites, including an accountability microsite, <http://www.aclu.org/accountability>; and a video series. The ACLU also regularly issues press releases to call attention to documents obtained through FOIA requests, as well as other breaking news. ACLU attorneys are interviewed frequently for news stories about documents released through ACLU FOIA requests.⁴

The ACLU website specifically includes features on information about actual or alleged government activity obtained through FOIA.⁵ For example, the ACLU maintains an online archive of surveillance-related documents released via FOIA as well as other sources.⁶ Similarly, the ACLU maintains an online “Torture Database,” which is a compilation of over 100,000 FOIA documents that allows researchers and the public to conduct sophisticated searches of FOIA documents relating to government policies on rendition, detention, and interrogation.⁷ The ACLU’s webpage concerning the Office of Legal Counsel torture memos obtained through FOIA contains commentary and analysis of the memos; an original, comprehensive chart summarizing the memos; links to web features created by ProPublica (an independent, non-profit, investigative-

⁴ *See, e.g.*, Nicky Woolf, *US Marshals Spent \$10M on Equipment for Warrantless Stingray Device*, *Guardian*, Mar. 17, 2016 (quoting ACLU attorney Nate Wessler); Peter Finn & Julie Tate, *CIA Mistaken on ‘High-Value’ Detainee, Document Shows*, *Wash. Post*, June 16, 2009 (quoting ACLU attorney Ben Wizner).

⁵ *See, e.g.*, <http://www.aclu.org/safefree/nsaspying/30022res20060207.html>; <http://www.aclu.org/mappingthefbi>; <http://www.aclu.org/patriotfoia>; <http://www.aclu.org/safefree/nationalsecurityletters/32140res20071011.html>.

⁶ <https://www.aclu.org/nsa-documents-search>.

⁷ <http://www.torturedatabase.org>.

journalism organization) based on the ACLU's information gathering, research, and analysis; and ACLU videos about the memos.⁸ In addition to its websites, the ACLU has produced an in-depth television series on civil liberties, which has included analysis and explanation of information the ACLU has obtained through FOIA.

Similarly, the ACLU of Northern California actively disseminates and frequently garners extensive media coverage of the information it obtains about actual or alleged government activity through FOIA and California's statutory counterpart, the California Public Records Act. It does so through a heavily visited website (averaging between 10,000 and 20,000 visitors per week) and a paper newsletter distributed to its members, who now number over 80,000. In the past, information obtained by the ACLU-NC through FOIA requests concerning government surveillance practices have garnered extensive national coverage.⁹ ACLU-NC staff persons are frequent spokespersons in television and print media and make frequent public presentations at meetings and events.

The ACLU plans to analyze and disseminate to the public the information gathered through this Request. The records requested are not sought for commercial use, and the Requesters plan to disseminate the information disclosed as a result of this Request to the public at no cost.¹⁰

⁸ http://www.aclu.org/safefree/general/olc_memos.html.

⁹ See, e.g., <https://www.aclunc.org/blog/justice-department-emails-show-feds-were-less-explicit-judges-cell-phone-tracking-tool>; Jennifer Valentino-Devries, *Judges Questioned Use of Cellphone Tracking Devices*, Wall St. J. (Mar. 27, 2013); Ellen Nakashima, *Little-Known Surveillance Tool Raises Concerns by Judges, Privacy Activists*, Wash. Post (Mar. 27, 2013); Rory Carroll, *ACLU Challenges 'Stingray Surveillance' that Allows Police to Track Cellphones*, Guardian (Mar. 28, 2013); Shaun Waterman, *Can You Hear Me Now Feds Admit FBI Warrantless Cellphone Tracking 'Very Common'*, Wash. Times (Mar. 29, 2013); Kim Zetter, *Government Fights for Use of Spy Tool That Spoofs Cell Towers*, Wired (Mar. 29, 2013); J.D. Tuccille, *Feds Routinely Track Cell Phones Without Telling Judges*, Reason.com (Mar. 27, 2013); Josh Peterson, *DOJ Emails Show Feds Kept Judges in the Dark About Cellphone Tracking Device*, Daily Caller (Mar. 28, 2013); *ACLU: Feds Secretly Using Highly Invasive Spying Tool*, Wash. Post (Mar. 28, 2013); Ryan Gallagher, *Feds Accused of Hiding Information From Judges About Covert Cellphone Tracking Tool*, Slate.com, (Mar. 28, 2013); *Feds Admit FBI Warrantless Cellphone Tracking 'Very Common,'* Press TV (Mar. 30, 2013); Vanessa Blum, *Emails Detail Northern District's Use of Controversial Surveillance*, Recorder (Apr. 1, 2013).

¹⁰ In addition to the national ACLU offices, there are 53 ACLU affiliate and national chapter offices located throughout the United States and Puerto Rico. These offices further disseminate ACLU material to local residents, schools, and organizations through a variety of means, including their own websites, publications, and newsletters.

B. The records sought are urgently needed to inform the public about actual or alleged government activity.

The records sought are urgently needed to inform the public. They relate to matters in which there is “[a]n urgency to inform the public about an actual or alleged Federal Government activity,” 28 C.F.R. § 16.5(e)(1)(ii), as well as matters “of widespread and exceptional media interest in which there exist possible questions about the government’s integrity which affect public confidence,” *id.* § 16.5(e)(1)(iv).

The records sought pertain to the government’s interpretation and implementation of surveillance laws that have drawn public scrutiny and significantly impact Americans’ privacy and free speech rights. In particular, they pertain to the Department of Justice’s use of information derived from surveillance under FISA and Title III in criminal prosecutions and other legal proceedings. This information is vitally needed to inform the ongoing public and congressional debate about whether the government’s electronic surveillance powers should be narrowed, whether Section 702 of FISA should be reauthorized in its current form when it expires this year, and whether Congress should act to strengthen existing notice requirements. Indeed, despite the government’s failure to properly provide notice of surveillance in the past, little remains known about how the government interprets its duty to provide notice of surveillance to Americans.

The government’s electronic surveillance powers have been a significant matter of public concern and media interest for many years, particularly after the revelation of the NSA’s warrantless wiretapping program. The legislation that emerged out of that controversy—Section 702 of FISA—has been the subject of widespread interest and debate since the moment it was introduced in 2008. *See, e.g.*, Sean Lengell, *House Approves Update of Bipartisan Spy Laws*, Wash. Times, June 21, 2008; Editorial, *Mr. Bush v. the Bill of Rights*, N.Y. Times, June 18, 2008; Editorial, *Compromising the Constitution*, N.Y. Times, July 8, 2008 (stating that the FAA would “make it easier to spy on Americans at home, reduce the courts’ powers and grant immunity to the companies that turned over Americans’ private communications without warrant”); Editorial, *Election-Year Spying Deal is Flawed, Overly Broad*, USA Today, June 25, 2008.

This public debate has only grown with recent disclosures concerning the scope and intrusiveness of government surveillance. Scores of articles published during the past three years have addressed the government’s surveillance activities—under FISA, Section 702, and Title III. *See, e.g.*, Barton Gellman et al., *In NSA-Intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are*, Wash. Post, (July 5, 2014), <http://wapo.st/1xyyGZF>; Charlie Savage, *N.S.A. Said to Search Content of Messages to and from U.S.*, N.Y. Times (Aug. 8, 2013), <http://nyti.ms/1ppBBoT>; Charlie Savage & Nicole Perloff, *Yahoo Said to Have Aided U.S. Email Surveillance by Adapting Spam*

Filter, N.Y. Times (Oct. 5, 2016), <http://nyti.ms/2jeRXx7>; Brad Heath & Brett Kelman, *Police Used Apparently Illegal Wiretaps to Make Hundreds of Arrests*, USA Today (Nov. 19, 2015), <http://usat.ly/1IEJmoF>.

A number of those articles have highlighted pressing concerns about whether the government is properly interpreting its obligation to provide notice of foreign-intelligence surveillance to criminal defendants and others. *See, e.g.*, Adam Liptak, *A Secret Surveillance Program Proves Challengeable in Theory Only*, N.Y. Times, July 15, 2013, <http://nyti.ms/12ANzNM>; Charlie Savage, *Door May Open for Challenge to Secret Wiretaps*, N.Y. Times, Oct. 16, 2013, <http://nyti.ms/1bAe7QZ>. That concern became particularly acute in the aftermath of the Supreme Court’s decision in *Clapper v. Amnesty Int’l USA*, 133 S. Ct. 1138 (2013), when it became apparent that the Department of Justice had not been providing notice to criminal defendants as expressly required by statute. *See, e.g.*, Devlin Barrett, *U.S. Spy Program Lifts Veil in Court*, Wall St. J., July 31, 2013, <http://on.wsj.com/19nu8KC>. Revelations of this failure have drawn intense public attention because, after *Clapper*, criminal prosecutions are one of the few avenues for obtaining judicial review of surveillance programs that affect thousands or even millions of Americans. *See* Scott Lemieux, *Secret Wiretapping Cannot Be Challenged Because It’s Secret*, The American Prospect, Feb. 26, 2013; Adam Liptak, *Justices Turn Back Challenge to Broader U.S. Eavesdropping*, N.Y. Times, Feb. 26, 2013. Indeed, both the Supreme Court and the Executive Branch indicated in *Clapper* that the proper avenue for judicial review of wiretapping activities is a criminal or administrative proceeding where the fruit of that surveillance is at issue. *See Clapper*, 133 S. Ct. 1138. Judicial review is impossible, however, unless criminal defendants and others receive notice of these searches. The request seeks information concerning Department of Justice policies and legal interpretations that bear directly on this matter of public concern.

As these events and sustained media interest clearly show, there is “[a]n urgency to inform the public about an actual or alleged Federal Government activity,” 28 C.F.R. § 16.5(e)(1)(ii), and the government’s use of information obtained or derived from foreign-intelligence surveillance constitutes a “matter of widespread and exceptional media interest in which there exist possible questions about the government’s integrity which affect public confidence,” 28 C.F.R. § 16.5(d)(1)(iv). The Request will inform an urgent and ongoing debate about the government’s surveillance and wiretapping activities.

Accordingly, expedited processing should be granted.

III. Application for Waiver or Limitation of Fees

A. Release of the records is in the public interest.

We request a waiver of search, review, and reproduction fees on the grounds that disclosure of the requested records is in the public interest because

it is likely to contribute significantly to the public understanding of the United States government's operations or activities and is not primarily in the commercial interest of the requester. 5 U.S.C. § 552(a)(4)(A)(iii); 28 C.F.R. § 16.11(k).

As discussed above, numerous news accounts reflect the considerable public interest in the requested records. Given the ongoing and widespread media attention to this issue, the records sought by the Request will significantly contribute to the public understanding of the operations and activities the agencies that are responsible for implementing Section 702. *See* 28 C.F.R. § 16.11(k)(1)(i). In addition, disclosure is not in the ACLU's commercial interest. As described above, any information disclosed as a part of this FOIA Request will be available to the public at no cost. Thus, a fee waiver would fulfill Congress's legislative intent in amending FOIA. *See Judicial Watch Inc. v. Rossotti*, 326 F.3d 1309, 1312 (D.C. Cir. 2003) ("Congress amended FOIA to ensure that it be 'liberally construed in favor of waivers for noncommercial requesters.'") (citation omitted); OPEN Government Act of 2007, Pub. L. No. 110-175, § 2, 121 Stat. 2524 (finding that "disclosure, not secrecy, is the dominant objective of the Act," quoting *Dep't of Air Force v. Rose*, 425 U.S. 352, 361 (1992)).

B. The ACLU qualifies as a representative of the news media.

A waiver of search and review fees is warranted because the ACLU qualifies as a "representative of the news media" and the requested records are not sought for commercial use. 5 U.S.C. § 552(a)(4)(A)(ii); *see also* 28 C.F.R. § 16.11(k). Accordingly, fees associated with the processing of this request should be "limited to reasonable standard charges for document duplication."

The ACLU meets the statutory and regulatory definitions of a "representative of the news media" because it is an "entity that gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw materials into a distinct work, and distributes that work to an audience." 5 U.S.C. § 552(a)(4)(A)(ii)(II); *see also Nat'l Sec. Archive v. Dep't of Def.*, 880 F.2d 1381, 1387 (D.C. Cir. 1989); *cf. ACLU v. Dep't of Justice*, 321 F. Supp. 2d 24, 30 n.5 (D.D.C. 2004) (finding non-profit public interest group to be "primarily engaged in disseminating information"). The ACLU is a "representative of the news media" for the same reasons that it is "primarily engaged in the dissemination of information." *See Elec. Privacy Info. Ctr. v. Dep't of Def.*, 241 F. Supp. 2d 5, 10–15 (D.D.C. 2003) (finding non-profit public interest group that disseminated an electronic newsletter and published books was a "representative of the news media" for FOIA purposes). The ACLU recently was held to be a "representative of the news media." *Serv. Women's Action Network v. Dep't of Def.*, No. 3:11CV1534 (MRK), 2012 WL 3683399, at *3 (D. Conn. May 14, 2012); *see also ACLU of Wash. v. Dep't of Justice*, No. C09–0642RSL, 2011 WL 887731, at *10 (W.D. Wash. Mar. 10, 2011) (finding ACLU of Washington to be a "representative of the news

media”), *reconsidered in part on other grounds*, 2011 WL 1900140 (W.D. Wash. May 19, 2011).¹¹

* * *

Pursuant to applicable statute and regulations, we expect a determination regarding expedited processing within ten (10) calendar days. *See* 5 U.S.C. § 552(a)(6)(E)(ii)(I); 28 C.F.R. § 16.5(e)(4).

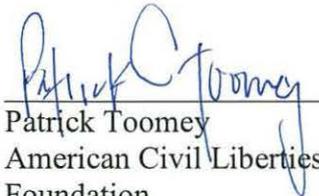
If the request is denied in whole or in part, we ask that you justify all withholdings by reference to specific exemptions to the FOIA. We also ask that you release all segregable portions of otherwise exempt material in accordance with 5 U.S.C. § 552(b). Furthermore, if any documents responsive to this request are classified, please identify those documents, including a date and document number where possible, so we may begin the process of requesting a Mandatory Declassification Review under the terms of Executive Order 13,526.

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

I certify that the foregoing information provided in support of the request for expedited processing is true and correct to the best of my knowledge and belief.

Executed on the 6th day of February, 2017.

Sincerely,



Patrick Toomey
American Civil Liberties Union
Foundation
125 Broad Street, 18th floor
New York, NY 10004
Tel: 212 549 2607
Fax: 212 549 2654
ptoomey@aclu.org

¹¹ In October 2015, the Department of State granted a fee waiver with respect to a request for documents relating to Executive Order 12,333. In October 2013, the Department of State granted a fee waiver with respect to a request for documents relating to the government’s targeted-killing program. In April 2013, the DOJ National Security Division granted a fee waiver with respect to a request for documents relating to the FISA Amendments Act. Also in April 2013, the DOJ granted a fee waiver with respect to a FOIA request for documents related to national security letters issued under the Electronic Communications Privacy Act. In August 2013, the FBI granted a fee waiver request related to the same FOIA request issued to the DOJ.

Exhibit 2

From: [NSDFOIA \(NSD\)](#)
To: [Patrick Toomey](#)
Subject: NSD FOIA Request #17-064
Date: Friday, February 10, 2017 3:04:42 PM
Attachments: [image001.gif](#)
[image002.jpg](#)
[image003.png](#)

Patrick Toomey
National Security Project
American Civil Liberties Union
125 Broad Street
New York, NY 10004

Re: FOIA/PA #17-064

Dear Mr. Toomey:

This is to acknowledge receipt of your email dated February 6, 2017 pertaining to 1. The memorandum titled "Determining Whether Evidence Is 'Derived From' Surveillance Under Title III or FISA,"³ as well as: a. Any cover letter or other document attached to this memorandum; b. Any version of this memorandum created or distributed on or after November 23, 2016, whether considered "final" or otherwise; and c. Any record modifying, supplementing, superseding, or rescinding this memorandum or its contents. Our FOIA office received your Freedom of Information Act request on February 6, 2017.

In response to your request, we have conducted a search of Office of the Assistant Attorney General for the National Security Division (NSD). We have located two records and processed these under the FOIA. We are withholding the records (as described on the enclosed schedule) in full pursuant to one or more of the following FOIA exemptions set forth in 5 U.S.C. 552(b):

(5) which permits the withholding of inter-agency or intra-agency memorandums or letters which reflect the predecisional, deliberative processes of the Department; and/or which consist of attorney work product prepared in anticipation of litigation; and,

(6) which permits the withholding of personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy; and,

(7) which permits the withholding of records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information...

(c) could reasonably be expected to constitute an unwarranted invasion of personal privacy.

If you are not satisfied with my response to this request, you may administratively appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, Suite 11050,

1425 New York Avenue, NW, Washington, DC 20530-0001, or you may submit an appeal through OIP's FOIAonline portal by creating an account on the following web site: <https://foiaonline.regulations.gov/foia/action/public/home>. Your appeal must be postmarked or electronically transmitted within 90 days of the date of my response to your request. If you submit your appeal by mail, both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal."

Sincerely,
Arnetta Mallory
Government Information Specialist

SCHEDULE OF DOCUMENTS WITHHELD IN FULL
(Refer to Body of Letter for Full Description of Each Exemption)

1. Memo 11-23-2016 Patty Merkamp Stemler, Chief, Appellate Section, Criminal Division and an NSD Attorney to All Federal Prosecutors; 2 pages.
Withheld in full pursuant to 5 U.S.C 552(b)(5).
Withheld in full pursuant to 5 U.S.C. 552 (b)(6) and (7)(C)
2. Determining Whether Evidence is "Derived From" Surveillance Under Title III or FISA; 31 pages.
Withheld in full pursuant to 5 U.S.C. 552 (b)(5).

From: Patrick Toomey [mailto:ptoomey@aclu.org]
Sent: Monday, February 06, 2017 10:14 AM
To: NSDFOIA (NSD) <Ex_NSDFoia@jmd.usdoj.gov>
Subject: FOIA Request / Expedited Processing Requested

Hello,

Please see the attached FOIA request, which includes a request for expedited processing.

Thank you for your prompt attention to this request.

Sincerely,
Patrick Toomey

Patrick Toomey

Staff Attorney, National Security Project

American Civil Liberties Union

125 Broad St., New York, NY 10004

| 212.519.7816 | ptoomey@aclu.org

www.aclu.org



This message may contain information that is confidential or legally privileged. If you are not the intended recipient, please immediately advise the sender by reply email that this message has been inadvertently transmitted to you and delete this email from your system.

Exhibit 3

LEGAL DEPARTMENT



February 22, 2017

VIA FOIA ONLINE

Director, Office of Information Policy (OIP)
U.S. Department of Justice
Suite 11050
1425 New York Ave., NW
Washington, DC 20530-0001

**RE: FREEDOM OF INFORMATION ACT APPEAL
FOIA TRACKING NO. 17-064**

To Whom It May Concern:

The American Civil Liberties Union, the American Civil Liberties Union Foundation, and the American Civil Liberties Union of Northern California (collectively, the “ACLU”) write to appeal the National Security Division’s response to Freedom of Information Act (“FOIA”) request number 17-064 (the “Request”) (Exhibit 1), in which the ACLU seeks disclosure of Department of Justice documents describing the circumstances in which the Department of Justice considers information or evidence to be “derived from” surreptitious surveillance, including surveillance conducted under the Foreign Intelligence Surveillance Act (“FISA”) and the Wiretap Act (“Title III”).

Specifically, the Request seeks:

1. The memorandum titled “Determining Whether Evidence Is ‘Derived From’ Surveillance Under Title III or FISA,”¹ as well as:
 - a. Any cover letter or other document attached to this memorandum;
 - b. Any version of this memorandum created or distributed on or after November 23, 2016, whether considered “final” or otherwise; and
 - c. Any record modifying, supplementing, superseding, or rescinding this memorandum or its contents.

¹ The ACLU understands that a final version of this document was distributed within the Department of Justice (DOJ) on November 23, 2016.

**AMERICAN CIVIL LIBERTIES
UNION FOUNDATION**
NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500
WWW.ACLU.ORG

OFFICERS AND DIRECTORS
SUSAN N. HERMAN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

ROBERT B. REMAR
TREASURER

The National Security Division (“NSD”) transmitted its final response to the ACLU via email on February 10, 2017 (“Response”) (Exhibit 2). NSD’s response states that it searched the Office of the Assistant Attorney General for the National Security Division and that it is withholding two memoranda in full pursuant to Exemption 5 (based on the deliberative-process and attorney work-product privileges), Exemption 6, and Exemption 7(C). *See* 5 U.S.C. § 552(b)(5)–(7).

The ACLU appeals from NSD’s response, both because its search for records was inadequate and because it has failed to justify its withholding of the two memoranda.

* * *

I. Inadequate Search

A. Scope of Search

The ACLU challenges the adequacy of NSD’s search. NSD’s response states that it conducted a search in the Office of the Assistant Attorney General, however, NSD does not appear to have searched other offices within the component. For example, NSD’s Office of Intelligence, which evaluates the legal authority for operations under FISA, and its Law and Policy Office, which provides assistance and advice on national security law, are also likely to have materials responsive to the Request and have been searched in response to similar requests in the past. *See, e.g.*, Decl. of Mark Bradley, *ACLU v. DOJ*, No. 13-cv-0747 (S.D.N.Y. Nov. 23, 2015) (ECF No. 49).

More broadly, NSD has provided no information about the manner in which it searched its files for responsive records. For example, the Response does not describe the types of records encompassed by NSD’s search; the repositories searched, whether classified or unclassified; the electronic search terms and protocols used, if any; or the individuals within NSD whom were consulted in order to identify responsive records. Without information about the manner in which NSD carried out its search, it is impossible to determine whether NSD’s search was reasonable and adequate.

II. Improper Withholding

A. Exemption 5

With respect to Exemption 5, although NSD states that the documents may be withheld pursuant to the deliberative-process and the attorney work-product privileges, it provides no facts whatsoever to support this conclusion, let alone the detailed description that courts require to sustain an invocation of these privileges. *See, e.g.*, *Automobile Club of N.Y. v. Port of N.Y. and N.J.*, 297 F.R.D. 55, 60 (S.D.N.Y. May 8, 2013) (applying *Nat’l Council of La Raza v. DOJ*, 411 F.3d 350

(2d Cir. 2005)); *United States v. Construction Products Research, Inc.*, 73 F.3d 464, 474 (2d Cir. 1996). Significantly, both documents appear to be final memoranda, and both were likely distributed as legal and policy guidance to “all federal prosecutors” in 93 U.S. Attorneys’ Offices across the country.² Response at 1. Despite NSD’s invocation of privilege, it has not described the decisionmaking process that the documents purportedly concern or how the documents relate to that process. It has not described the specific claim and litigation for which the documents were purportedly prepared. And it has not identified who received the documents, or how those individuals used and relied on them. Because NSD has not provided these basic details and others, it is impossible to conclude that the documents meet the basic elements of these privileges—for instance, that they are “predecisional” and “deliberative,” or that they were prepared in reasonable anticipation of specific litigation.

NSD has also failed to establish that the two withheld records do not contain “working law” or adopted law and policy. Disclosure of working law and adopted law and policy is required under FOIA notwithstanding any invocation of privilege. *See, e.g., Brennan Ctr. for Justice v. DOJ*, 697 F.3d 184, 195–208 (2d Cir. 2012); 5 U.S.C. § 552(a). Both of the withheld records are likely to contain information reflecting the government’s effective law and policy—precisely because the Request sought legal analysis and memoranda, as well as any cover letter or other attachments. OIP has previously concluded, in response to a similar request, that NSD improperly sought to withhold policy memoranda in full where disclosure was in fact required. *See* OIP Response Letter dated Aug. 25, 2016 (Appeal No. DOJ-AP-2016-000457).

A. Exemption 6 and 7(C)

With respect to Exemptions 6 and 7(C), NSD’s response does not identify or describe the portions of the documents that have been withheld on the basis of these exemptions. As a result, it is impossible to conclude that the withheld information properly falls within the asserted exemptions. However, based on the nature of the Request, it is extremely unlikely that records at issue are “personnel and medical files and similar files” that would qualify for Exemption 6 protection at all. 5 U.S.C. § 552(b)(6). Instead, they are legal and policy memoranda providing guidance on DOJ’s use of evidence derived from surveillance conducted under FISA and Title III. Similarly, NSD has not established that the records were compiled for “law enforcement purposes” nor does it point to any information therein whose disclosure “could reasonably be expected to constitute an unwarranted invasion of personal privacy.” *Id.* § 552(b)(7).

B. Segregability

² Notably, NSD does not identify either of the withheld documents as “drafts,” though that label alone would not establish that the memoranda may be withheld under FOIA.

Finally, NSD has not shown that it attempted to segregate all non-exempt information in the records, including statements of fact and descriptions of existing policy, as FOIA requires. *See* 5 U.S.C. § 552(b). Merely invoking privilege and citing Exemption 5, 6, and 7(C) does not relieve NSD's burden to show that the documents were reviewed for segregable information.

Because NSD has not provided sufficient information about the withheld records and the basis for their withholding, it has not met its burden of establishing that the records are exempt under FOIA.

* * *

For the foregoing reasons, NSD should be required to conduct an adequate search and release the two withheld documents responsive to the Request.

Thank you for your prompt attention to this matter.

Sincerely,

/s/ Patrick Toomey

Patrick Toomey
American Civil Liberties Union
Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
ptoomey@aclu.org

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

Exhibit 4



U.S. Department of Justice
Office of Information Policy
Suite 11050
1425 New York Avenue, NW
Washington, DC 20530-0001

Telephone: (202) 514-3642

March 17, 2017

Patrick C. Toomey, Esq.
American Civil Liberties Union
Foundation
18th Floor
125 Broad Street
New York, NY 10004
ptoomey@aclu.org

Re: Appeal No. DOJ-AP-2017-002487
Request No. 17-064
MWH:RNB

VIA: FOIAonline

Dear Mr. Toomey:

You appealed on behalf of your clients, the American Civil Liberties Union, the American Civil Liberties Union Foundation, and the American Civil Liberties Union of Northern California, from the action of the National Security Division (NSD) on your clients' Freedom of Information Act request for access to certain records concerning the memorandum titled "Determining Whether Evidence Is 'Derived From' Surveillance Under Title III or FISA".

After carefully considering your appeal, I am affirming, on partly modified grounds, NSD's action on your request. The FOIA provides for disclosure of many agency records. At the same time, Congress included in the FOIA nine exemptions from disclosure that provide protection for important interests such as personal privacy, privileged communications, and certain law enforcement activities. NSD properly withheld this information in full because it is protected from disclosure under the FOIA pursuant to:

5 U.S.C. § 552(b)(5), which concerns certain inter- and intra-agency records protected by the attorney work-product privilege;

5 U.S.C. § 552(b)(6), which concerns material the release of which would constitute a clearly unwarranted invasion of the personal privacy of third parties; and

5 U.S.C. § 552(b)(7)(C), which concerns records or information compiled for law enforcement purposes the release of which could reasonably be expected to constitute an unwarranted invasion of the personal privacy of third parties.

Please be advised that for each of these exemptions, it is reasonably foreseeable that disclosure of the information withheld would harm the interests protected by these exemptions.

- 2 -

As to your appeal concerning the adequacy of NSD's search for responsive records subject to the FOIA, I have determined that NSD's response was correct and that it conducted an adequate, reasonable search for such records. NSD searched the offices reasonably likely to maintain records responsive to your request.

Please be advised that this Office's decision was made only after a full review of this matter. Your appeal was assigned to an attorney with this Office who thoroughly reviewed and analyzed your appeal, your clients' underlying request, and the action of NSD on your clients' request. If you have any questions regarding the action this Office has taken on your appeal, you may contact this Office's FOIA Public Liaison for your appeal. Specifically, you may speak with the undersigned agency official by calling (202) 514-3642.

If your clients are dissatisfied with my action on your appeal, the FOIA permits them to file a lawsuit in federal district court in accordance with 5 U.S.C. § 552(a)(4)(B).

For your information, the Office of Government Information Services (OGIS) offers mediation services to resolve disputes between FOIA requesters and Federal agencies as a non-exclusive alternative to litigation. Using OGIS services does not affect your clients' right to pursue litigation. The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, Room 2510, 8601 Adelphi Road, College Park, Maryland 20740-6001; e-mail at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

Sincerely,

X 

Sean R. O'Neill
Chief, Administrative Appeals Staff

Exhibit 5

STATISTICAL TRANSPARENCY REPORT
REGARDING USE OF NATIONAL SECURITY AUTHORITIES
FOR CALENDAR YEAR 2016

April 2017

Introduction

In June 2014, the Director of National Intelligence (DNI) began releasing statistics relating to the use of critical national security authorities, including the Foreign Intelligence Surveillance Act (FISA), in an annual report called the *Statistical Transparency Report Regarding Use of National Security Authorities* (hereafter the *Annual Statistical Transparency Report*). Subsequent *Annual Statistical Transparency Reports* were released in 2015 and 2016.

On June 2, 2015, the USA FREEDOM Act was enacted, codifying a requirement to publicly report many of the statistics already reported in the *Annual Statistical Transparency Report*. The Act also expanded the scope of the information included in the reports by requiring the DNI to report information concerning United States person search terms and queries of certain FISA-acquired information, as well as specific statistics concerning information collected pursuant to call detail records. See 50 U.S.C. § 1873(b).

Today, consistent with the USA FREEDOM Act requirements to release certain statistics (codified in 50 U.S.C. § 1873(b)) and the Intelligence Community's (IC) *Principles of Intelligence Transparency*, we are releasing our **fourth** *Annual Statistical Transparency Report* presenting statistics on how often the government uses certain national security authorities.

This fourth report has been reformatted to provide a description of the statistics being reported. Related definitions and additional context to the statistics included in this report are provided throughout. The order in which the statistics are presented remains consistent with last year's report and follows the order set forth in 50 U.S.C. § 1873(b).

Additional public information on national security authorities is available at the Office of the Director of National Intelligence's (ODNI) website, www.dni.gov, and ODNI's public tumblr site, IContheRecord.tumblr.com.

FISA Title I -- Title III -- Title VII Sections 703 & 704

→ *All of these authorities require individual court orders based on probable cause.*

→ *Titles I and III apply to FISA activities directed against persons within the United States.*

→ *Sections 703 and 704 apply to FISA activities directed against U.S. persons outside the United States.*

Both FISA Title I and FISA Title III require a probable cause court order to target individuals within the United States regardless of U.S. person status. Under FISA, Title I permits electronic surveillance and Title III permits physical search in the United States of foreign powers or agents of a foreign power for the purpose of collecting foreign intelligence information. *See* 50 U.S.C. §§ 1804 and 1823. Title I (electronic surveillance) and Title III (physical search) are commonly referred to as “Traditional FISA.” Both require that the Foreign Intelligence Surveillance Court (FISC) make a probable cause finding, based upon a factual statement in the government’s application, that (i) the target is a foreign power or an agent of a foreign power, as defined by FISA and (ii) the facility being targeted for electronic surveillance is used by or about to be used, or the premises or property to be searched is or is about to be owned, used, possessed by, or is in transit to or from a foreign power or an agent of a foreign power. In addition to meeting the probable cause standard, the government’s application must meet the other requirements of FISA. *See* 50 U.S.C. §§ 1804(a) and 1823(a).

FISA Title VII Sections 703 and 704 similarly require a court order based on a finding of probable cause for the government to undertake FISA activities targeting U.S. persons located outside the United States. Section 703 applies when the government seeks to conduct electronic surveillance or to acquire stored electronic communications or stored electronic data, in a manner that otherwise requires an order pursuant to FISA, of a U.S. person who is reasonably believed to be located outside the United States. Section 704 applies when the government seeks to conduct collection overseas targeting a U.S. person reasonably believed to be located outside the United States under circumstances in which the U.S. person has a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted in the United States. Both Sections 703 and 704 require that the FISC make a probable cause finding, based upon a factual statement in the government’s application, that

the target is a U.S. person reasonably believed to be (i) located outside the United States and (ii) a foreign power, agent of a foreign power, or officer or employee of a foreign power; additionally, the government's application must meet the other requirements of FISA. See 50 U.S.C. §§ 1881b(b) and 1881c(b).

- **U.S. Person.** As defined by Title I of FISA, a U.S. person is “a citizen of the United States or an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act), an unincorporated association with a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in [50 U.S.C. § 1801(a)(1), (2), or (3)].” 50 U.S.C. § 1801(i). Section 602 of the USA FREEDOM Act, however, uses a narrower definition. Since the broader Title I definition governs how U.S. person queries are conducted pursuant to the relevant minimization procedures, it will be used throughout this report.
- **Target.** Within the IC, the term “target” has multiple meanings. With respect to the statistics provided in this report, the term “target” is defined as the individual person, group, entity composed of multiple individuals, or foreign power that uses the selector such as a telephone number or email address.

The role of the FISC. If the FISC finds that the government's application meets the requirements of FISA and the Constitution, the FISC must issue an order approving the requested authority.

- **Types of Orders.** There are different types of orders that the FISC may issue in connection with FISA cases, for example: orders granting or modifying the government's authority to conduct intelligence collection; orders directing electronic communication service providers to provide any technical assistance necessary to implement the authorized intelligence collection; and supplemental orders and briefing orders requiring the government to take a particular action or provide the court with specific information.
- **Amendments and Renewals.** The FISC may amend an order one or more times after it has been issued. For example, an order may be amended to add a newly discovered account used by the target. This report does not count such amendments separately. The FISC may renew some orders multiple times during the calendar year. Each authority permitted under FISA has specific time limits for the FISA authority to continue (e.g., a Section 704 order against a U.S. person target may last no longer than 90 days

but FISA permits the order to be renewed, see 50 U.S.C. § 1881c(c)(4)). Each renewal requires a separate application submitted by the government to the FISC and a finding by the FISC that the application meets the requirements of FISA. Thus, unlike amendments, this report does count each such renewal as a separate order. These terms will be used consistently throughout this report.

FISA “Probable Cause” Court Orders and Targets

<u>Titles I and III and Sections 703 and 704 of FISA</u>	CY2013	CY2014	CY2015	CY2016
Total number of orders	1,767	1,519	1,585	1,559
Estimated* number of targets of such orders	1,144	1,562	1,695	1,687

See 50 U.S.C. § 1873(b)(1).

*Throughout this report, when numbers are *estimated*, the estimate comports with the statutory requirements to provide a “good faith estimate” of a particular number.

How targets are counted. If the IC received authorization to conduct electronic surveillance and/or physical search against the same target in four separate applications, the IC would count one target, not four. Alternatively, if the IC received authorization to conduct electronic surveillance and/or physical search against four targets in the same application, the IC would count four targets. Duplicate targets across authorities are not counted.

FISA “Probable Cause” Targets – U.S. Persons*

<u>Titles I and III and Sections 703 and 704 -- Targets</u>	CY2016
Estimated number of targets who are <i>non</i> -U.S. persons	1,351
Estimated number of targets who are U.S. persons	336
Estimated percentage of targets who are U.S. persons	19.9%

*While not statutorily required to publicly provide these statistics, the IC is providing them consistent with the commitment to its *Principles of Intelligence Transparency*.

Title VII - FISA Amendment Act (FAA) Section 702

→ *Commonly referred to as “Section 702.”*

→ *Requires individual targeting determinations that the target is (1) a non-United States person who (2) is reasonably believed to be located outside the United States and who (3) has or is expected to communicate or receive foreign intelligence information.*

Section 702. Title VII of FISA includes Section 702, which permits the Attorney General and the DNI to jointly authorize the targeting of (i) non-U.S. persons reasonably believed to be (ii) located outside the United States to (iii) acquire foreign intelligence information. See 50 U.S.C. § 1881a. All three elements must be met. Additionally, Section 702 requires that the Attorney General, in consultation with the DNI, adopt targeting procedures and minimization procedures that they attest satisfy the statutory requirements and are consistent with the Fourth Amendment.

- **Section 702 Targets and “Tasking.”** Under Section 702, the government “targets” a particular non-U.S. person, group, or entity reasonably believed to be located outside the United States and who possesses, or who is likely to communicate or receive, foreign intelligence information, by directing an acquisition at – i.e., “tasking” – selectors (e.g., telephone numbers and email addresses) that are assessed to be used by such non-U.S. person, group, or entity, pursuant to targeting procedures approved by the FISC.

Before “tasking” a selector for collection under Section 702, the government must apply its targeting procedures to ensure that the IC appropriately tasks a selector used by a non-U.S. person who is reasonably believed to be located outside the United States and who will likely possess, communicate, or receive foreign intelligence information.

The FISC’s role. Under Section 702, the FISC determines whether *certifications* provided jointly by the Attorney General and the DNI appropriately meet all the requirements of Section 702. If the FISC determines that the government’s certifications and its targeting and minimization procedures meet the statutory requirements of Section 702 and are consistent with the Fourth Amendment, then the FISC issues an order and supporting statement approving the certifications. A recent FISC order and statement approving certifications was publicly released in April 2016 and posted on *IC on the Record*.

- **Certifications.** The certifications are jointly executed by the Attorney General and DNI and authorize the government to acquire foreign intelligence information under Section 702. Each annual certification application package must be submitted to the FISC for approval. The package includes the Attorney General and DNI's certifications, affidavits by certain heads of intelligence agencies, targeting procedures, and minimization procedures. A sample of a certification application package was publicly released on *IC on the Record*. The certifications identify categories of information to be collected, which must meet the statutory definition of foreign intelligence information, through the targeting of non-U.S. persons reasonably believed to be located outside the United States. The certifications have included information concerning international terrorism and other topics, such as the acquisition of information concerning weapons of mass destruction.
- **Targeting procedures.** The targeting procedures detail the steps that the government must take before tasking a selector, as well as verification steps after tasking, to ensure that the user of the tasked selector is being targeted appropriately – specifically, that the user is a non-U.S. person, located outside the United States, who is being tasked to acquire foreign intelligence information. The IC must make individual determinations that each tasked selector meets the requirements of the targeting procedures. As part of the certification package, the FISC reviews the sufficiency of the IC's targeting procedures, which includes assessing the IC's compliance with the procedures.
- **Minimization procedures.** The minimization procedures detail requirements the government must meet to use, retain, and disseminate Section 702 data, which include specific restrictions on how the IC handles non-publicly available U.S. person information acquired from Section 702 collection of non-U.S. person targets, consistent with the needs of the government to obtain, produce, and disseminate foreign intelligence information. As part of the certification package, the FISC reviews the sufficiency of the IC's minimization procedures, which includes assessing the IC's compliance with past procedures. The 2015 minimization procedures have been released on *IC on the Record*.

The IC's adherence to the targeting and minimization procedures is subject to robust internal agency oversight and to rigorous external oversight by the Department of Justice (DOJ), ODNI, Congress, and the FISC. Every identified incidence of non-compliance is reported to the FISC (through individual notices or in reports) and to Congress in semiannual reports. DOJ and ODNI also submit semiannual reports to Congress that assess the IC's overall compliance efforts. Past assessments have been publicly released.

Section 702 Orders

<u>Section 702 of FISA</u>	CY2013	CY2014	CY2015	CY2016
Total number of orders issued	1	1	1	0

See 50 U.S.C. § 1873(b)(2).

Counting Section 702 orders. As explained above, the FISC may issue a single order to approve more than one Section 702 certification to acquire foreign intelligence information.

Note that, in its own transparency report, which is required pursuant to 50 U.S.C. § 1873(a), the Director of the Administrative Office of the United States Courts (AOUSC) counted each of the Section 702 certifications associated with the FISC's order. Because the number of the government's Section 702 certifications remains a classified fact, the government requested that the AOUSC redact the number of certifications from its transparency report prior to publicly releasing it.

In 2016, the government submitted a certification application to the FISC. Pursuant to 50 U.S.C. § 1881a(j)(2), the FISC extended its review of the 2016 certifications. The FISC may extend its review of the certifications "as necessary for good cause in a manner consistent with national security." See 50 U.S.C. § 1881a(j)(2). Thus, because the FISC did not complete its review of the 2016 certifications during calendar year 2016, the FISC did not issue an order concerning those certifications in calendar year 2016. The 2015 order remained in effect during the extension period.

Section 702 Targets*

<u>Section 702 of FISA</u>	CY2013	CY2014	CY2015	CY2016
Estimated number of targets of such orders	89,138	92,707	94,368	106,469

*While there is no statutory requirement to disclose this number, it is provided in this report to foster public understanding of the IC's use of the Section 702 collection authority. The IC is committed to sharing as much information as possible with the public without jeopardizing mission capabilities.

Estimating Section 702 targets. The number of 702 "targets," provided above, reflects an estimate of the number of non-United States persons who are the users of tasked selectors. This estimate is based on information readily available to the IC. Unless and until the IC has information that links multiple selectors to a single foreign intelligence target, each individual

selector is counted as a separate target for purposes of this report. On the other hand, where the IC is aware that multiple selectors are used by the same target, the IC counts the user of those selectors as a single target. This counting methodology reduces the risk that the IC might inadvertently understate the number of discrete persons targeted pursuant to Section 702.

Section 702 Search Terms Used to Query Content

<u>Section 702 of FISA</u>	CY2015	CY2016
Estimated number of search terms concerning a known U.S. person used to retrieve the unminimized contents of communications obtained under Section 702 (excluding search terms used to prevent the return of U.S. person information)*	4,672	5,288

See 50 U.S.C. § 1873(b)(2)(A).

*Consistent with § 1873(d)(2)(A), this statistic does not include queries that are conducted by the Federal Bureau of Investigation (FBI).

The above is the good faith estimate of the number of *search terms* (e.g., email addresses and telephone numbers,) concerning known U.S. persons that the government used to query unminimized (i.e., raw) lawfully acquired Section 702 *content*.

Counting U.S. person *search terms* used to query Section 702 *content*. The National Security Agency (NSA) counts the number of U.S. person identifiers it uses to query the content of unminimized Section 702-acquired information. For example, if the NSA used U.S. person identifier “johndoe@XYXprovider” to query the content of Section 702-acquired information, the NSA would count it as one regardless of how many times the NSA used “johndoe@XYXprovider” to query its 702-acquired information. In calendar year 2016, the Central Intelligence Agency (CIA) adopted this same model for counting search terms. In prior calendar years, however, the CIA counted the total number of actual queries it conducted using U.S. person identifiers. For example, if the CIA used the identifier “johndoe@XYXprovider” 7 times, in prior years the CIA would count this as 7 search terms. Now, CIA the counts this as a single search term.

Section 702 Queries of Noncontents

<u>Section 702 of FISA</u>	CY2013	CY2014	CY2015	CY2016
Estimated number of queries concerning a known U.S. person of unminimized noncontents information obtained under Section 702 (excluding queries containing information used to prevent the return of U.S. person information)*	9500	17,500	23,800	30,355

See 50 U.S.C. § 1873(b)(2)(B).

*Consistent with § 1873(d)(2)(A), this statistic does not include queries that are conducted by the FBI.

The above is a good faith estimate of the number of *queries* concerning a known U.S. person that the government conducted of unminimized (i.e., raw) lawfully acquired Section 702 *metadata*.

Counting *queries* using U.S. person identifiers of noncontents collected under Section 702.

This estimate represents the number of times a U.S. person identifier is used to query the noncontents (i.e., metadata) of unminimized Section 702-acquired information. For example, if the U.S. person identifier telephone number “111-111-2222” was used 15 times to query the noncontents of Section 702-acquired information, the number of queries counted would be 15.

As with last year’s transparency report, one IC element remains currently unable to provide the number of queries using U.S. person identifiers of unminimized Section 702 noncontent information. Under 50 U.S.C. § 1873(d)(3)(A), if the DNI concludes that this good-faith estimate cannot be determined accurately because not all of the relevant elements of the IC are able to provide this good faith estimate, then the DNI is required to (i) certify that conclusion in writing to the relevant Congressional committees; (ii) report the good faith estimate for those relevant elements able to provide such good faith estimate; (iii) explain when it is reasonably anticipated that such an estimate will be able to be determined fully and accurately; and (iv) make such certification publicly available on an Internet web site. Because one IC element remains unable to provide such information, the DNI made a certification, pursuant to § 1873(d)(3)(A) to the relevant Congressional committees.

As required by statute, this certification is being made publicly available as an attached appendix to this current report (see Appendix A).

Required Section 702 Query Reporting to the FISC

<u>Section 702 of FISA</u>	CY2016
Per the FISC Memorandum Opinion and Order dated November 6, 2015: Each instance in which FBI personnel <i>received and reviewed</i> Section 702-acquired information that the FBI identified as concerning a U.S. person in response to a query that was designed to return evidence of a crime unrelated to foreign intelligence.	1

On November 6, 2015, the FISC granted the government’s application for renewal of the 2015 certifications and, among other things, concluded that the FBI’s U.S. person querying provisions in its minimization procedures, “strike a reasonable balance between the privacy interests of the United States persons and persons in the United States, on the one hand, and the government’s national security interests, on the other.” *Memorandum Opinion and Order* dated November 6, 2015, at 44 (released on *IC on the Record* on April 19, 2016). The FISC further stated that the FBI conducting queries, “designed to return evidence of crimes unrelated to foreign intelligence does not preclude the Court from concluding that taken together, the targeting and minimization procedures submitted with the 2015 Certifications are consistent with the requirements of the Fourth Amendment.” *Id.*

Nevertheless, the FISC ordered the government to report in writing, “each instance after December 4, 2015, in which FBI personnel *receive and review* Section 702-acquired information that the FBI identifies as concerning a United States person in response to a query that is not designed to find and extract foreign intelligence information.” (Emphasis added). *Id.* at 44 and 78. The FISC directed that the report contain details of the query terms, the basis for conducting the query, the manner in which the query will be or has been used, and other details. *Id.* at 78. In keeping with the *IC’s Principles of Transparency*, the DNI declassified the number of each instance such queries occurred in calendar year 2016.

**ADDITIONAL SECTION 702 STATISTICS
PROVIDED IN
RESPONSE TO PCLOB RECOMMENDATION 9(5)**

In July 2014, the Privacy and Civil Liberties Oversight Board (PCLOB or Board) issued a report on Section 702 entitled, “Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act” (*PCLOB’s Section 702 Report*), which contained 10 recommendations. Recommendation 9 focused on “accountability and transparency,” noting that the government should implement measures, “to provide insight about the extent to which the NSA acquires and utilizes the communications involving U.S. persons and people located in the United States under the Section 702 program.” *PCLOB’s Section 702 Report* at 145-146. Specifically, the PCLOB recommended that “the NSA should implement processes to annually count [...] (5) the number of instances in which the NSA disseminates non-public information about U.S. persons, specifically distinguishing disseminations that includes names, titles, or other identifiers potentially associated with individuals.” *Id.* at 146. This recommendation is commonly referred to as Recommendation 9(5). In response to Recommendation 9(5), NSA previously publicly provided (in the *Annual Statistical Transparency Report* for calendar year 2015) and continues to provide the following additional information regarding the dissemination of Section 702 intelligence reports that contain U.S. person information.

NSA has been providing similar information to Congress per FISA reporting requirements. For example, FISA Section 702(l)(3) requires that NSA annually submit a report to applicable Congressional committees regarding certain numbers pertaining to the acquisition of Section 702-acquired information, including the number of “disseminated intelligence reports containing a reference to a United States person identity.” *See* 50 U.S.C. § 1881(l)(3)(A)(i). Additionally, NSA provides this number to Congress as part of Attorney General and Director of National Intelligence’s joint assessment of compliance. *See* 50 U.S.C. § 1881(l)(1).

Prior to the PCLOB issuing its *Section 702 Report*, NSA’s Director of Civil Liberties and Privacy Office published *NSA’s Implementation of Foreign Intelligence Surveillance Act Section 702*,” on April 16, 2014, (hereinafter “NSA DCLPO Report”), in which it explained NSA’s dissemination processes. *NSA DCLPO Report* at 7-8. NSA “only generates classified intelligence reports when the information meets a specific intelligence requirement, regardless of whether the proposed report contains U.S. person information.” *NSA DCLPO Report* at 7.

- **Dissemination.** In the most basic sense, dissemination refers to the sharing of minimized information. As it pertains to FISA (including Section 702), if an agency (in this instance NSA) lawfully collects information pursuant to FISA and wants to share (i.e., disseminate) that information, the agency must first apply its minimization procedures to that information.

Section 702 only permits the targeting of non-U.S. persons reasonably believed to be located outside the United States to acquire foreign intelligence information. Such targets, however, may communicate information to, from, or about U.S. persons. NSA minimization procedures (publicly released on August 11, 2016) permit the NSA to disseminate U.S. person information if the NSA masks the information that could identify the U.S. person. The minimization procedures permit NSA to disseminate the U.S. person identity only if doing so meets one of the specified reasons listed in NSA's minimization procedures, including that the U.S. person consented to the dissemination, the U.S. person information was already publicly available, the U.S. person identity was necessary to understand foreign intelligence information, or the communication contained evidence of a crime and is being disseminated to law enforcement authorities. Even if one of these conditions applies, as a matter of policy, NSA may still mask the U.S. person information and will include no more than the minimum amount of U.S. person information necessary to understand the foreign intelligence or to describe the crime or threat. *Id.* In certain instances, however, NSA makes a determination prior to releasing its original classified report that the U.S. person's identity is appropriate to disseminate in the first instance using the same standards discussed above.

- **Masked U.S. Person Information.** Information about a U.S. person is masked when the identifying information about the person is not included in a report. For example, instead of reporting that Section 702-acquired information revealed that non-U.S. person "Bad Guy" communicated with U.S. person "John Doe" (i.e., the actual name of the U.S. person), the report would mask "John Doe's" identity, and would state that "Bad Guy" communicated with "an identified U.S. person," "a named U.S. person," or "a U.S. person."

Recipients of NSA's classified reports, such as other Federal agencies, may request that NSA provide the true identity of a masked U.S. person referenced in an intelligence report. The requested identity information is released only if the requesting recipient has a legitimate "need to know" the identity of the U.S. person and has the appropriate security clearances, and if the dissemination of the U.S. person's identity would be consistent with NSA's minimization procedures (e.g., the identity is necessary to understand foreign intelligence information or assess its importance). Furthermore, per NSA policy, NSA is allowed to unmask the identity for

the specific requesting recipient only where specific additional controls are in place to preclude its further dissemination and additional approval has been provided by a designated NSA official.

As part of their regular oversight reviews, DOJ and ODNI review disseminations of information about U.S. persons that NSA obtained pursuant to Section 702 to ensure that the disseminations were performed in compliance with the minimization procedures.

<u>Section 702 – U.S. person (USP) information disseminated by NSA</u>	CY2016
Total number of NSA disseminated §702 Reports containing USP identities	3,914
Of those NSA disseminated §702 Reports containing USP identities (from the first row in this chart), the USP identity was originally <i>masked</i> in this many reports	2,964*
Of those NSA disseminated §702 Reports containing USP identities (from the first row in this chart), the USP identity was originally <i>revealed</i> in this many reports	1,200*
Of those NSA disseminated §702 Reports containing USP identities where the USP identities was originally masked (from the second row in this chart), the number of USP identities that NSA later released in response to specific requests to unmask a USP identity**	1,934

*A single report may contain both masked and unmasked U.S. person identities.

**For this statistic, last year's Annual Statistical Transparency Report provided the number of approved *requests* (i.e., 654) for unmasking of U.S. person identities, rather than the number of U.S. person identities that were released. A single request may contain multiple U.S. person identities. This year's report provides the number of U.S. person identities referred to by name or title released in response to specific requests to unmask those identities. The number of U.S. person identities that NSA released during calendar year 2015 in response to specific requests to unmask an identity was 2,232, which was the number that should have been reported in last year's report.

FISA Title IV – USE of PEN REGISTER and TRAP and TRACE (PR/TT) DEVICES

→ Commonly referred to as the “PR/TT” provision.

→ Bulk collection is prohibited.

→ Requires individual FISC order to use PR/TT device to capture dialing, routing, addressing, or signaling (DRAS) information.

→ Government request to use a PR/TT device on U.S. person target must be based on an investigation to protect against terrorism or clandestine intelligence activities and that investigation must not be based solely on the basis of activities protected by the First Amendment to the Constitution.

Pen Register/Trap and Trace Authority. Title IV of FISA authorizes the use of pen register and trap and trace (PR/TT) devices for foreign intelligence purposes. Title IV authorizes the government to use a PR/TT device to seek and capture dialing, routing, addressing or signaling (DRAS) information. The government may submit an application to the FISC for an order approving use of a PR/TT device (i.e., PR/TT order) for (i) “any investigation to obtain foreign intelligence information not concerning a United States person or” (ii) “to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a U.S. person is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution.” 50 U.S.C. § 1842(a). If the FISC finds that the government’s application sufficiently meets the requirements of FISA, the FISC must issue an order for the installation and use of a PR/TT device.

PR/TT Statistics

<u>Title IV of FISA</u> <i>PR/TT FISA</i>	CY2013	CY2014	CY2015	CY2016
Total number of orders	131	135	90	60
Estimated number of targets of such orders	319	516	456	41
Estimated number of unique identifiers used to communicate information collected pursuant to such orders*	-	-	134,987**	125,378

See 50 U.S.C. §§ 1873(b)(3), 1873(b)(3)(A), and 1873(b)(3)(B).

*Pursuant to §1873(d)(2)(B), this statistic does not apply to orders resulting in the acquisition of information by the FBI that does not include electronic mail addresses or telephone numbers.

**This number represents information the government received from provider(s) electronically for the entire 2015 calendar year. The government does not have a process for capturing unique identifiers received by other means (such as hard-copy or portable media).

Counting orders. Similar to how orders were counted for Titles I and III and Sections 703 and 704, this report only counts the orders *granting authority to conduct intelligence collection* -- the order for the installation and use of a PR/TT device. Thus, renewal orders are counted as a separate order; modification orders and amendments are not counted.

Estimating the number of targets. The government's methodology for counting PR/TT targets is similar to the methodology described above for counting targets of electronic surveillance and/or physical search. If the IC received authorization for the installation and use of a PR/TT device against the same target in four separate applications, the IC would count one target, not four. Alternatively, if the IC received authorization for the installation and use of a PR/TT device against four targets in the same application, the IC would count four targets.

Estimating the number of unique identifiers. This statistic counts (1) the targeted identifiers and (2) the non-targeted identifiers (e.g., telephone numbers and e-mail addresses) that were in contact with the targeted identifiers. Specifically, the House Report on the USA FREEDOM Act states that "[t]he phrase 'unique identifiers used to communicate information collected pursuant to such orders' means the total number of, for example, email addresses or phone numbers that have been collected as a result of these particular types of FISA orders--not just

the number of target email addresses or phone numbers." [H.R. Rept. 114-109 Part I, p. 26], with certain exceptions noted.

FISA PR/TT Targets – U.S. Persons*

<u>PR/TT Targets</u>	CY2016
Estimated number of targets who are <i>non</i> -U.S. persons	23
Estimated number of targets who are U.S. persons	18
Estimated percentage of targets who are U.S. persons	43.9%

*While not statutorily required to publicly provide these statistics, the IC is providing them consistent with the *Principles of Intelligence Transparency*.

The remainder of this page is intentionally left blank.

FISA Title V – BUSINESS RECORDS

→ Commonly referred to as “Business Records” provision.

→ Bulk collection is prohibited.

→ Call Detail Records (CDR) may be obtained from a telephone company if the FISC issues an individual court order for target’s records.

→ Request for records in an investigation of a U.S. person must be based on an investigation to protect against terrorism or clandestine intelligence activities and provided that the investigation is not conducted solely upon activities protected by the First Amendment to the Constitution.

Business Records FISA. Under FISA, Title V authorizes the government to submit an application for an order requiring the production of any tangible things for (i) “an investigation to obtain foreign intelligence information not concerning a U.S. person or” (ii) “to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a U.S. person is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution.” 50 U.S.C. § 1861. Title V is commonly referred to as the “Business Records” provision of FISA.

In June 2015, the USA FREEDOM Act was signed into law and, among other things, amended Title V, including prohibiting bulk collection. See 50 U.S.C. §§ 1861(b), 1861(k)(4). The DNI is required to report various statistics about two Title V provisions – traditional business records and call detail records (discussed further below).

On November 28, 2015, in compliance with amendments enacted by the USA FREEDOM Act, the IC terminated collection of bulk telephony metadata under Title V of the FISA (the “Section 215 Program”). Solely due to legal obligations to preserve records in certain pending civil litigation, including *First Unitarian Church of Los Angeles, et al. v. National Security Agency, et al.*, No. C 13-03287-JSW (N.D. Cal.) and *Jewel, et al. v. National Security Agency, et al.*, No. C 08-04373-JSW (N.D. Cal.), the IC continues to preserve previously collected bulk telephony metadata. Under the terms of a FISC order dated November 24, 2015, the bulk telephony metadata cannot be used or accessed for any purpose other than compliance with preservation obligations. Once the government’s preservation obligations are lifted, the government is

required to promptly destroy all bulk metadata produced by telecommunications providers under the Section 215 Program.

As noted in last year's *Annual Statistical Transparency Report*, on November 30, 2015, the IC implemented certain provisions of the USA FREEDOM Act, including the call detail records provision and the requirement to use a specific selection term. Accordingly, only one month's worth of data for calendar year 2015 was available with respect to those provisions. Any statistical information relating to a particular FISA authority for a particular month remains classified. Therefore, the Title V data specifically associated with December 2015 was only released in a classified annex provided to Congress as part of the report for CY2015. For this CY 2016 report, statistical information was collected for an entire year under the USA FREEDOM Act Title V provisions. As a result, those statistics are included in this report.

Statistics related to *traditional business records* under Title V Section 501(b)(2)(B) are provided first pursuant to 50 U.S.C. § 1873(b)(4). Statistics related to *call detail records* under Title V Section 501(b)(2)(C) are provided second pursuant to 50 U.S.C. § 1873(b)(5).

“Traditional” Business Records – Section 501(b)(2)(B)

Business Record (BR) requests for tangible things include books, records, papers, documents, and other items pursuant to 50 U.S.C. §1861(b)(2)(B), also referred to as Section 501(b)(2)(B) . These are commonly referred to as “Traditional” Business Records.

“Traditional” Business Records Statistics

Business Records “BR” – Section 501(b)(2)(B)	CY2016
Total number of orders issued pursuant to applications under Section 501(b)(2)(B)	84
Estimated number of targets of such orders	88
Estimated number of unique identifiers used to communicate information collected pursuant to such orders	81,035

See 50 U.S.C. §§ 1873(b)(4), 1873(b)(4)(A), and 1873(b)(4)(B).

Estimating the number of unique identifiers. This is an estimate of the number of (1) targeted identifiers (e.g., telephone numbers and email addresses) and (2) non-targeted identifiers that were in contact with the targeted identifiers. This metric represents unique identifiers received

electronically from the provider(s). The government does not have a process for capturing unique identifiers received by other means (i.e., hard-copy or portable media).

Explaining how we count BR statistics. As an example of the government’s methodology, assume that in 2016, the government submitted a BR request targeting “John Doe” with email addresses john.doe@serviceproviderX, john.doe@serviceproviderY, and john.doe@serviceproviderZ. The FISC found that the application met the requirements of Title V and issued orders granting the application and directing service providers X, Y, and Z to produce business records pursuant to Section 501(b)(2)(B). Provider X returned 10 non-targeted email addresses that were in contact with the target; provider Y returned 10 non-targeted email addresses that were in contact with the target; and provider Z returned 10 non-targeted email addresses that were in contact with the target. Based on this scenario, we would report the following statistics: A) one order by the FISC for the production of tangible things, B) one target of said orders, and C) 33 unique identifiers, representing three targeted email addresses plus 30 non-targeted email addresses.

Call Detail Records – Section 501(b)(2)(C)

Call Detail Records (CDR) – commonly referred to as “call event metadata” – may be obtained from telecommunications providers pursuant to 50 U.S.C. §1861(b)(2)(C). A CDR is defined as session identifying information (including an originating or terminating telephone number, an International Mobile Subscriber Identity (IMSI) number, or an International Mobile Station Equipment Identity (IMEI) number), a telephone calling card number, or the time or duration of a call. *See* 50 U.S.C. §1861(k)(3)(A). CDRs do not include the content of any communication, the name, address, or financial information of a subscriber or customer, or cell site location or global positioning system information. *See* 50 U.S.C. §1861(k)(3)(B). CDRs are stored and queried by the service providers. *See* 50 U.S.C. §1861(c)(2).

Call Detail Record (CDR) Statistics

Call Detail Records “CDR” – Section 501(b)(2)(C)	CY2016
Total number of orders issued pursuant to applications under Section 501(b)(2)(C)	40
Estimated number of targets of such orders	42

See 50 U.S.C. §§ 1873(b)(5) and 1873(b)(5)(A).

Estimating the number of targets of CDR orders. A “target” is the person using the selector. For example, if a target uses four selectors that have been approved, the number counted for purposes of this report would be one target, not four. Alternatively, if two targets are using one selector that has been approved, the number counted would be two targets.

The estimated number of Call Detail Records received from providers. This metric represents the number of *records received* from the provider(s) and stored in NSA repositories (records that fail at any of a variety of validation steps are not included in this number). CDRs covered by § 501(b)(2)(C) include call detail records created before, on, or after the date of the application relating to an authorized investigation. While the USA FREEDOM Act directs the government to provide a good faith estimate of “the number of unique identifiers used to communicate information collected pursuant to” orders issued in response to CDR applications (see § 1873(b)(5)(B)), the statistic below does *not* reflect the number of unique identifiers contained within the call detail records received from the providers. As of the date of this report, the government does not have the technical ability to isolate the number of unique identifiers within records received from the providers. As explained in the 2016 NSA’s public report on the USA FREEDOM Act, the metric provided is over-inclusive because the government counts each record *separately even if the government receives the same record multiple times* (whether from one provider or multiple providers). Additionally, this metric includes duplicates of unique identifiers – i.e., because the government lacks the technical ability to isolate unique identifiers, the statistic counts the number of records even if unique identifiers are repeated. This statistic includes records that were received from the providers in CY2016 for all orders active for any portion of the year, which includes orders that the FISC approved in 2015.

Call Detail Record (CDR) Statistics

Call Detail Records “CDR” – Section 501(b)(2)(C)	CY2016
Estimated number of call detail records received from providers and stored in NSA repositories	151,230,968

As an example, assume an NSA intelligence analyst learns that phone number (202) 555-1234 is being used by a suspected international terrorist. This is the “specific selection term” or “selector” that will be submitted to the FISC (or the Attorney General in an emergency) for approval using the “reasonable articulable suspicion” (RAS) standard. Assume that one provider (provider X) submits to NSA a record showing (202) 555-1234 had called (301) 555-4321 on May 1, 2016. This is the “first hop” and would count as one record. If the provider submits records showing additional calls between those same telephone numbers, each would count as an

additional record. Thus, if over the course of 2016, (202) 555-1234 was in contact with (301) 555-4321 once each day, then that would count as 365 records obtained from provider X. If another provider (provider Y) also submits records showing direct contact between those two telephone numbers (assume the same number of contacts), then those would add to the count.

In turn, assume that NSA submits the “first-hop” number above – (301) 555-4321- to the providers, and finds that it was used to call (410) 555-5678. This is the “second-hop” result. Each contact between the first-hop and second-hop numbers would count as a separate record, as would each such contact submitted by other providers. More information on how NSA implements this authority can be found in the DCLPO report.

Call Detail Record (CDR) Statistics

Call Detail Records “CDR” – Section 501(b)(2)(C)	CY2016
Estimated number of search terms that included information concerning a U.S. person that were used to query any database of call detail records obtained through the use of such orders*	22,360

See 50 U.S.C. § 1873(b)(5)(C).

*Consistent with § 1873(d)(2)(A), this statistic does not include queries that are conducted by the FBI.

The number of search terms associated with a U.S. person used to query the CDR data. Each unique query is counted only once. The same term queried 10 times, still counts as one search term. Similarly, a single query with 20 terms counts as 20.

The remainder of this page is intentionally left blank.

NATIONAL SECURITY LETTERS (NSLs)

→ Not authorized by FISA but by other statutes.

→ Bulk collection is prohibited, however, by the USA FREEDOM Act.

→ FBI may only use NSLs if the information sought is relevant to international counterterrorism or counterintelligence investigation.

National Security Letters. In addition to statistics relating to FISA authorities, we are reporting information on the government's use of National Security Letters (NSLs). The FBI is statutorily authorized to issue NSLs for specific records (as specified below) only if the information being sought is relevant to a national security investigation. NSLs may be issued for four commonly used types of records:

- 1) telephone subscriber information, toll records, and other electronic communication transactional records, see 18 U.S.C. § 2709;
- 2) consumer-identifying information possessed by consumer reporting agencies (names, addresses, places of employment, institutions at which a consumer has maintained an account), see 15 U.S.C. § 1681u;
- 3) full credit reports, see 15 U.S.C. § 1681v (only for counterterrorism, not for counterintelligence investigations); and
- 4) financial records, see 12 U.S.C. § 3414.

Counting NSLs. Today we are reporting (1) the total number of NSLs *issued* for all persons, and (2) the total number of requests for information (ROI) contained within those NSLs. When a single NSL contains multiple requests for information, each is considered a "request" and each request must be relevant to the same pending investigation. For example, if the government issued one NSL seeking subscriber information from one provider and that NSL identified three e-mail addresses for the provider to return records, this would count as one NSL issued and three ROIs.

- **The Department of Justice's Report on NSLs.** In April 2017, the Department of Justice released its *Annual Foreign Intelligence Surveillance Act Report* to Congress. That report, which is available online, reports on the *number of requests* made for certain

information concerning different U.S. persons pursuant to NSL authorities during calendar year 2016. The Department of Justice's report provides the number of individuals subject to an NSL whereas the ODNI's report provides the number of NSLs issued. Because one person may be subject to more than one NSL in an annual period, the number of NSLs issued and the number of persons subject to an NSL differs.

Why we report the number of NSL requests instead of the number of NSL targets. We are reporting the annual number of requests for multiple reasons. First, the FBI's systems are configured to comply with Congressional reporting requirements, which do not require the FBI to track the number of individuals or organizations that are the subject of an NSL. Even if the FBI systems were configured differently, it would still be difficult to identify the number of specific individuals or organizations that are the subjects of NSLs. One reason for this is that the subscriber information returned to the FBI in response to an NSL may identify, for example, one subscriber for three accounts or it may identify different subscribers for each account. In some cases this occurs because the identification information provided by the subscriber to the provider may not be true. For example, a subscriber may use a fictitious name or alias when creating the account. Thus, in many instances, the FBI never identifies the actual subscriber of a facility. In other cases, this occurs because individual subscribers may identify themselves differently for each account (e.g., inclusion of middle name, middle initial, etc.) when creating an account.

We also note that the actual number of individuals or organizations that are the subject of an NSL is different than the number of NSL requests. The FBI often issues NSLs under different legal authorities, e.g., 12 U.S.C. § 3414(a)(5), 15 U.S.C. §§ 1681u(a) and (b), 15 U.S.C. § 1681v, and 18 U.S.C. § 2709, for the same individual or organization. The FBI may also serve multiple NSLs for an individual for multiple facilities (e.g., multiple e-mail accounts, landline telephone numbers and cellular phone numbers). The number of requests, consequently, is significantly larger than the number of individuals or organizations that are the subjects of the NSLs.

NSL Statistics

<u>National Security Letters (NSLs)</u>	CY2013	CY2014	CY2015	CY2016
Total number of NSLs issued	19,212	16,348	12,870	12,150
Number of Requests for Information (ROI)	38,832	33,024	48,642	24,801

See 50 U.S.C. § 1873(b)(6).

APPENDIX A

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

APR 28 2017

The Honorable Richard Burr
Chairman
Select Committee on Intelligence
United States Senate

The Honorable Chuck Grassley
Chairman
Committee on the Judiciary
United States Senate

The Honorable Devin Nunes
Chairman
Permanent Select Committee on Intelligence
U.S. House of Representatives

The Honorable Robert W. Goodlatte
Chairman
Committee on the Judiciary
U.S. House of Representatives

Dear Messrs. Chairmen:

Section 603(b)(2)(B) of the *Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015*, (P.L.114-23), 129 Stat. 268 (hereinafter “USA FREEDOM Act”), requires the Director of National Intelligence (“DNI”) to make publicly available for the preceding 12-month period a good faith estimate of the number of queries concerning a known United States person of unminimized non-content information relating to electronic communications or wire communications obtained through acquisitions authorized under Section 702 of the Foreign Intelligence Surveillance Act (“FISA”), excluding the number of queries containing information used to prevent the return of information concerning a United States person.

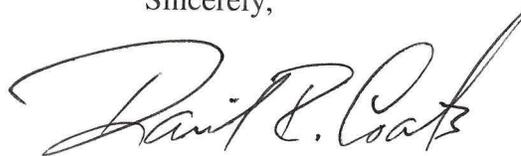
If the DNI concludes that this good faith estimate cannot be determined accurately because some, but not all, of the relevant elements of the Intelligence Community (“IC”) are able to provide such good faith estimate, the USA FREEDOM Act requires him to (i) certify that conclusion in writing to the committees identified above; (ii) report the good faith estimate for those relevant elements able to provide such good faith estimate; (iii) explain when it is reasonably anticipated that such an estimate will be able to be determined fully and accurately; and (iv) make such certification publicly available on an Internet website.

I conclude that the good faith estimate required under section 603(b)(2)(B) of the USA FREEDOM Act cannot be determined accurately because some but not all of the relevant elements of the IC are able to provide such good faith estimate. The enclosed report includes the good faith estimate for those relevant IC elements that were able to provide such good faith estimate. Based on the information provided to me by the relevant elements, I reasonably anticipate that such an estimate will be able to be determined fully and accurately by the end of calendar year 2018.

The Honorable Richard Burr
The Honorable Chuck Grassley
The Honorable Devin Nunes
The Honorable Robert W. Goodlatte

If you have any questions regarding this matter, please contact the Office of DNI Director of Legislative Affairs, Deirdre M. Walsh, at (703) 275-2474.

Sincerely,

A handwritten signature in black ink, appearing to read "Daniel R. Coats". The signature is fluid and cursive, with a prominent initial "D" and "C".

Daniel R. Coats

Enclosure:
Statistical Transparency Report

cc:

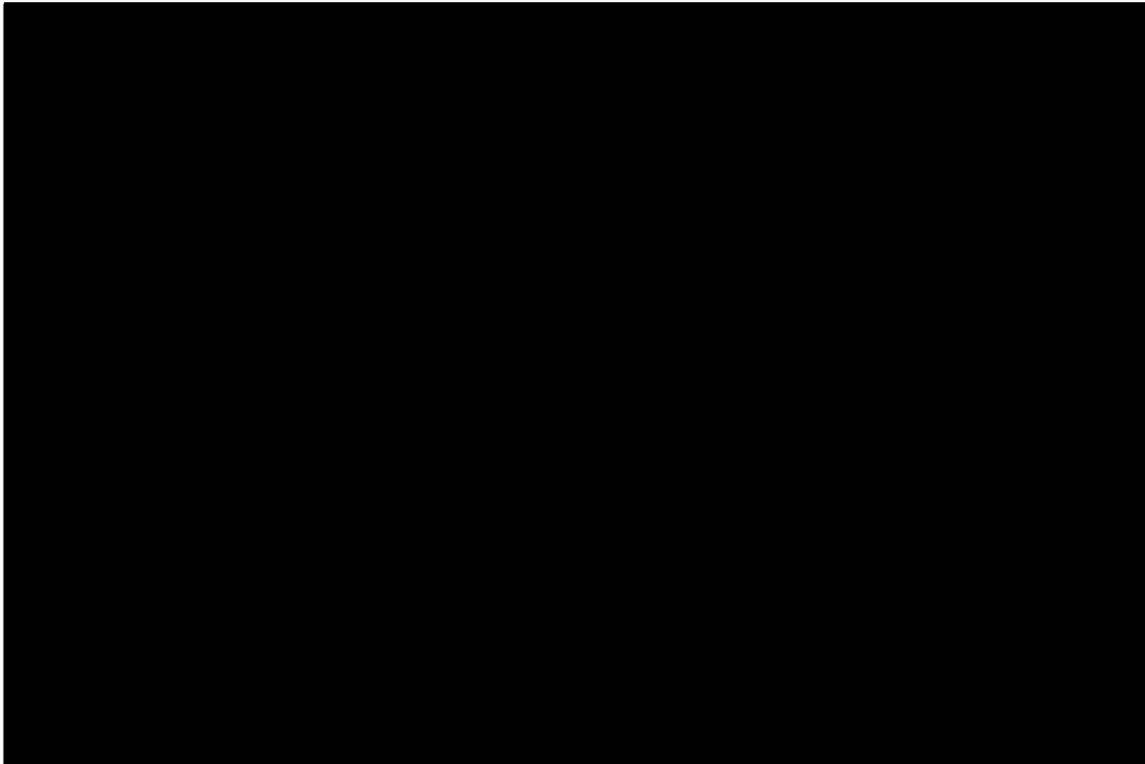


Exhibit 6

Wiretap Report 2016

Last updated on December 31, 2016

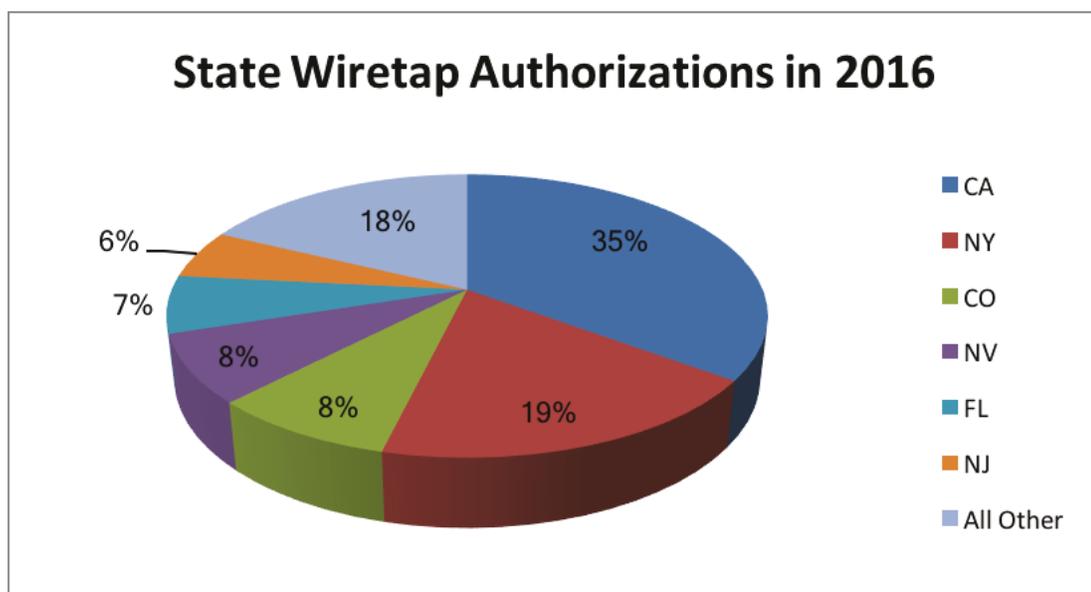
This report covers intercepts concluded between January 1, 2016, and December 31, 2016, as reported to the AO, and provides supplementary information reported to the AO on arrests and convictions resulting from intercepts concluded in prior years.

Forty-eight jurisdictions (the federal government, the District of Columbia, the Virgin Islands, Puerto Rico, and 44 states) currently have laws that authorize courts to issue orders permitting wire, oral, or electronic surveillance. [Table 1 \(/statistics/table/wire-1/wiretap/2016/12/31\)](#) shows that a total of 27 jurisdictions reported using at least one of these types of surveillance as an investigative tool during 2016.

Summary and Analysis of Reports by Judges

The number of federal and state wiretaps reported in 2016 decreased 24 percent from 2015. A total of 3,168 wiretaps were reported as authorized in 2016, with 1,551 authorized by federal judges and 1,617 authorized by state judges. Compared to the applications approved during 2015, the number approved by federal judges increased 11 percent in 2016, and the number approved by state judges decreased 41 percent. The largest reduction in reported state wiretap applications occurred in California, where 50 percent fewer applications were reported. Two wiretap applications were reported as denied in 2016.

In 26 states, a total of 107 separate local jurisdictions (including counties, cities, and judicial districts) reported wiretap applications for 2016. Applications concentrated in six states (California, New York, Colorado, Nevada, Florida, and New Jersey) accounted for 82 percent of all state wiretap applications. Applications in California alone constituted 35 percent of all applications approved by state judges.



Seventy-seven federal jurisdictions submitted reports of wiretap applications for 2016. For the third year in a row, the District of Arizona authorized the most federal wiretaps, approximately 9 percent of the applications approved by federal judges.

Federal judges and state judges reported the authorization of 600 wiretaps and 177 wiretaps, respectively, for which the AO received no corresponding data from prosecuting officials. Wiretap Tables [A-1 \(/statistics/table/wire-a1/wiretap/2016/12/31\)](#) and [B-1 \(/statistics/table/wire-b1/wiretap/2016/12/31\)](#) (which will become available online after July 1, 2017, at [http://www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports \(/statistics-reports/analysis-reports/wiretap-reports\)](http://www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports (/statistics-reports/analysis-reports/wiretap-reports))) contain information from judge and prosecutor reports submitted for 2016. The entry "NP" (no prosecutor's report) appears in these tables whenever a prosecutor's report was not submitted. Some prosecutors may have delayed filing reports to avoid jeopardizing ongoing investigations. Some of the prosecutors' reports require additional information to comply with reporting requirements or were received too late to include in this document. Information about these wiretaps should appear in future reports.

Intercept Orders, Extensions, and Locations

[Table 2 \(/statistics/table/wire-2/wiretap/2016/12/31\)](#) presents the number of intercept orders issued in each jurisdiction that provided reports, the number of extensions granted, the average lengths of the original periods authorized and any extensions, the total number of days in operation, and the locations of the communications intercepted. Federal and state laws limit the period of surveillance under an original order to 30 days. This period, however, can be lengthened by one or more extensions if the authorizing judge determines that additional time is justified.

During 2016, the average reported length of an original authorization was 30 days, the same as in 2015. The average reported length of an extension was also 30 days. In total, 2,096 extensions were reported as requested and authorized in 2016, a decrease of 36 percent from the prior year. The District of Arizona and the Middle District of Florida conducted the longest federal intercepts that were terminated in 2016. An original order in the District of Arizona was extended 10 times to complete a 306-day wiretap used in a narcotics investigation. In the Middle District of Florida, an order was extended nine times to complete a 290-day wiretap in a narcotics investigation. For state intercepts terminated in 2016, the longest intercepts occurred in Queens County, New York, where 2 original orders each were extended 30 times to complete both 457-day wiretaps used in a narcotics investigation.

The most frequently noted location in reported wiretap applications was "portable device." This category includes cell phone communications, text messages, and application software (apps). In 2016, a total of 93 percent of all authorized wiretaps (2,947 wiretaps) were reported to have used portable devices.

Prosecutors, under certain conditions, including a showing of probable cause to believe that actions taken by a party being investigated could have the effect of thwarting interception from a specified facility, may use "roving" wiretaps to target specific persons by using electronic devices at multiple locations rather than at a specific telephone or location (see 18 U.S.C § 2518(11)). In 2016, a total of 64 reported federal and state wiretaps were designated as roving.

Criminal Offenses

Drug offenses were the most prevalent type of criminal offenses investigated using reported wiretaps. [Table 3 \(/statistics/table/wire-3/wiretap/2016/12/31\)](#) indicates that 61 percent of all applications for intercepts (1,949 wiretap applications) in 2016 cited narcotics as the most serious offense under investigation. Applications citing narcotics plus those citing other offenses, which include other offenses related to drugs, accounted for 82 percent of all reported wiretap applications in 2016, compared to 84 percent in 2015. Conspiracy, the second-most frequently cited crime, was specified in 8 percent of applications. Homicide, the third-largest category, was specified as the most serious offense in approximately 5 percent of applications. Many applications for court orders revealed that multiple criminal offenses were under investigation, but [Table 3 \(/statistics/table/wire-3/wiretap/2016/12/31\)](#) includes only the most serious criminal offense listed on an application.

Lengths and Numbers of Intercepts

In 2016, for reported intercepts, installed wiretaps were in operation for an average of 44 days, 1 day longer than the average in 2015. The federal wiretap with the most intercepts occurred during a narcotics investigation in the Middle District of Pennsylvania and resulted in the interception of 3,292,385 cell phone conversations or messages over 60 days. The state wiretap with the most intercepts was a 118-day wiretap for a narcotics investigation in Los Angeles County, California, which resulted in the interception of 559,003 cell phone conversations, of which 113,528 were incriminating.

Encryption

The number of state wiretaps reported in which encryption was encountered increased from 7 in 2015 to 57 in 2016. In 48 of these wiretaps, officials were unable to decipher the plain text of the messages. A total of 68 federal wiretaps were reported as being encrypted in 2016, of which 53 could not be decrypted. Encryption was also reported for 20 federal and 19 state wiretaps that were conducted during a previous year, but reported to the AO for the first time in 2016. Officials were not able to decipher the plain text of the communications in any of the state intercepts or in 13 of the federal intercepts.

Cost of Intercepts

[Table 5 \(/statistics/table/wire-5/wiretap/2016/12/31\)](#) provides a summary of expenses related to wiretaps in 2016. The expenditures noted reflect the cost of installing intercept devices and monitoring communications for the 2,332 authorizations for which reports included cost data. The average cost of an intercept in 2016 was \$74,949, up 78 percent from the average cost in 2015. The most expensive state wiretap was in the Appellate Division of the Supreme Court, New York, where costs for a 434-day narcotics wiretap that resulted in 15 arrests and no convictions totaled \$2,989,930. For federal wiretaps for which expenses were reported in 2016, the average cost was \$83,356, a 70 percent increase from 2015. The most expensive federal wiretap completed during 2016 occurred in the Southern District of California, where costs for a narcotics investigation totaled \$5,266,558.

Methods of Surveillance

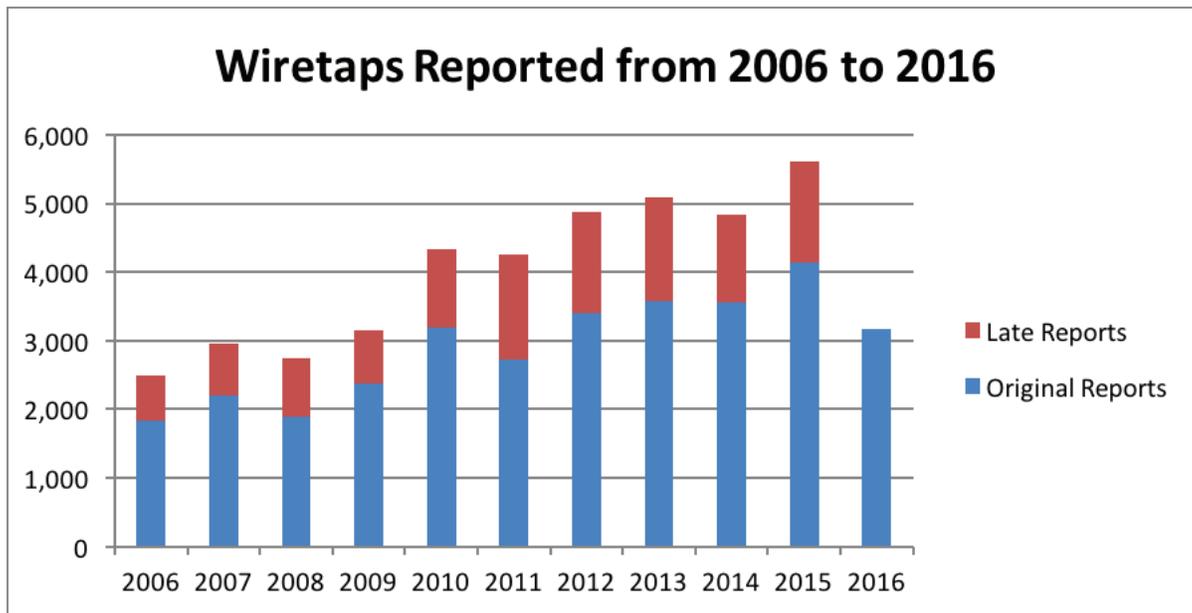
The three major categories of surveillance are wire, oral, and electronic communications. [Table 6 \(/statistics/table/wire-6/wiretap/2016/12/31\)](#) presents the type of surveillance method used for each intercept installed. The most common method reported was wire surveillance that used a telephone (land line, cellular, cordless, or mobile). Telephone wiretaps accounted for 84 percent (1,955 cases) of the intercepts installed in 2016, the majority of them involving cellular telephones.

Arrests and Convictions

Data on individuals arrested and convicted as a result of interceptions reported as terminated are presented in [Table 6 \(/statistics/table/wire-6/wiretap/2016/12/31\)](#). As of December 31, 2016, a total of 12,412 persons had been arrested (up 179 percent from 2015), and 1,248 persons had been convicted (up 112 percent from 2015). Federal wiretaps were responsible for 15 percent of the arrests and 7 percent of the convictions arising from wiretaps for this period. The Southern District of New York reported the most arrests for a federal district in 2016, with wiretaps there resulting in the arrest of 488 individuals. At the state level, Oklahoma Criminal Appeals reported the largest number of total arrests (5,057), followed by Queens County, New York (736). Queens County, New York, also had the highest number of total convictions (380) for any state jurisdiction in 2016.

Summary of Reports for Years Ending December 31, 2006, through December 31, 2016

[Table 7 \(/statistics/table/wire-7/wiretap/2016/12/31\)](#) presents data on intercepts reported each year from 2006 to 2016. Authorized intercept applications reported by year increased 72 percent from 1,839 in 2006 to 3,168 in 2016 (the total for 2006 was revised after initial publication). The majority of wiretaps have consistently been used for narcotics investigations, which accounted for 80 percent of intercepts initially reported in 2006 (1,473 applications) and 76 percent in 2016 (1,949 applications). [Table 9 \(/statistics/table/wire-9/wiretap/2016/12/31\)](#) presents the total number of arrests and convictions resulting from intercepts terminated in calendar years 2006 through 2016.



Supplementary Reports

Under 18 U.S.C. § 2519(2), prosecuting officials must file supplementary reports on additional court or police activity occurring as a result of intercepts reported in prior years. Because many wiretap orders are related to large-scale criminal investigations that cross county and state boundaries, supplemental reports are necessary to fulfill reporting requirements. Arrests, trials, and convictions resulting from these interceptions often do not occur within the same year in which the intercepts were first reported. [Table 8 \(/statistics/table/wire-8/wiretap/2016/12/31\)](#) shows that a total of 12,440 arrests, 6,694 convictions, and additional costs of \$201,427,611 arose from and were reported for wiretaps completed in previous years. Sixty percent of the supplementary reports of additional activity in 2016 involved wiretaps terminated in 2015. Interceptions concluded in 2015 led to 53 percent of arrests, 30 percent of convictions, and 40 percent of expenditures noted in the supplementary reports.

APPENDIX TABLES

Title	Publication Table Number	Reporting Period	Report Name	
Intercepts of Wire, Oral, or Electronic Communications Authorized by U.S. District Courts and Terminated	Wire A1	December 31, 2016	Wiretap	Download (XLSX, 496.07 KB)
Intercepts of Wire, Oral, or Electronic Communications Authorized by State Courts and Terminated	Wire B1	December 31, 2016	Wiretap	Download (XLSX, 321.12 KB)

WIRETAP

Title	Publication Table Number	Reporting Period	Report Name	
Jurisdictions with Statutes Authorizing the Interception of Wire, Oral, or Electronic Communications Effective	Wire 1	December 31, 2016	Wiretap	Download (XLSX, 12.19 KB)

Title	Publication Table Number	Reporting Period	Report Name	
Intercept Orders Issued by Judges	Wire 2	December 31, 2016	Wiretap	Download (XLSX, 37.24 KB)
Major Offenses for Which Court-Authorized Intercepts Were Granted	Wire 3	December 31, 2016	Wiretap	Download (XLSX, 24.85 KB)
Interceptions of Wire, Oral, or Electronic Communications	Wire 4	December 31, 2016	Wiretap	Download (XLSX, 22.75 KB)
Average Cost per Order	Wire 5	December 31, 2016	Wiretap	Download (XLSX, 18.28 KB)
Types of Surveillance Used, Arrests, and Convictions for Intercepts Installed	Wire 6	December 31, 2016	Wiretap	Download (XLSX, 22.6 KB)
Authorized Intercepts Granted	Wire 7	December 31, 2016	Wiretap	Download (XLSX, 16.03 KB)
Supplementary Data for Intercepts Terminated in Prior Years as Reported	Wire 8	December 31, 2016	Wiretap	Download (XLSX, 16.97 KB)
Arrests and Convictions Resulting from Intercepts Installed	Wire 9	December 31, 2016	Wiretap	Download (XLSX, 27.37 KB)

Exhibit 7

National Security

In NSA-intercepted data, those not targeted far outnumber the foreigners who are

Files provided by Snowden show extent to which ordinary Web users are caught in the net

By **Barton Gellman, Julie Tate and Ashkan Soltani** July 5, 2014

Ordinary Internet users, American and non-American alike, far outnumber legally targeted foreigners in the communications intercepted by the National Security Agency from U.S. digital networks, according to a four-month investigation by The Washington Post.

Nine of 10 account holders found in a large cache of intercepted conversations, which former NSA contractor Edward Snowden provided in full to The Post, were not the intended surveillance targets but were caught in a net the agency had cast for somebody else.

Many of them were Americans. Nearly half of the surveillance files, a strikingly high proportion, contained names, e-mail addresses or other details that the NSA marked as belonging to U.S. citizens or residents. NSA analysts masked, or “minimized,” more than 65,000 such references to protect Americans’ privacy, but The Post found nearly 900 additional e-mail addresses, unmasked in the files, that could be strongly linked to U.S. citizens or U.S. residents.

(How 160,000 intercepted conversations led to The Post’s latest NSA story)

The surveillance files highlight a policy dilemma that has been aired only abstractly in public. There are discoveries of considerable intelligence value in the intercepted messages — and collateral harm to privacy on a scale that the Obama administration has not been willing to address.

Among the most valuable contents — which The Post will not describe in detail, to avoid interfering with ongoing operations — are fresh revelations about a secret overseas nuclear project, double-dealing by an ostensible ally, a military calamity that

befell an unfriendly power, and the identities of aggressive intruders into U.S. computer networks.

Months of tracking communications across more than 50 alias accounts, the files show, led directly to the 2011 capture in Abbottabad of Muhammad Tahir Shahzad, a Pakistan-based bomb builder, and Umar Patek, a suspect in a 2002 terrorist bombing on the Indonesian island of Bali. At the request of CIA officials, The Post is withholding other examples that officials said would compromise ongoing operations.

(Transcript: Q&A with Barton Gellman)

Many other files, described as useless by the analysts but nonetheless retained, have a startlingly intimate, even voyeuristic quality. They tell stories of love and heartbreak, illicit sexual liaisons, mental-health crises, political and religious conversions, financial anxieties and disappointed hopes. The daily lives of more than 10,000 account holders who were not targeted are catalogued and recorded nevertheless.

In order to allow time for analysis and outside reporting, neither Snowden nor The Post has disclosed until now that he obtained and shared the content of intercepted communications. The cache Snowden provided came from domestic NSA operations under the broad authority granted by Congress in 2008 with amendments to the Foreign Intelligence Surveillance Act. FISA content is generally stored in closely controlled data repositories, and for more than a year, senior government officials have depicted it as beyond Snowden's reach.

The Post reviewed roughly 160,000 intercepted e-mail and instant-message conversations, some of them hundreds of pages long, and 7,900 documents taken from more than 11,000 online accounts.

The material spans President Obama's first term, from 2009 to 2012, a period of exponential growth for the NSA's domestic collection.

Taken together, the files offer an unprecedented vantage point on the changes wrought by Section 702 of the FISA amendments, which enabled the NSA to make freer use of methods that for 30 years had required probable cause and a warrant from a judge. One program, code-named PRISM, extracts content stored in user accounts at Yahoo, Microsoft, Facebook, Google and five other leading Internet companies. Another, known inside the NSA as Upstream, intercepts data on the move as it crosses the U.S. junctions of global voice and data networks.

No government oversight body, including the Justice Department, the Foreign Intelligence Surveillance Court, intelligence committees in Congress or the president's Privacy and Civil Liberties Oversight Board, has delved into a comparably large sample of what the NSA actually collects — not only from its targets but also from people who may cross a target's path.

Among the latter are medical records sent from one family member to another, résumés from job hunters and academic transcripts of schoolchildren. In one photo, a young girl in religious dress beams at a camera outside a mosque.

Scores of pictures show infants and toddlers in bathtubs, on swings, sprawled on their backs and kissed by their mothers. In some photos, men show off their physiques. In others, women model lingerie, leaning suggestively into a webcam or striking risqué poses in shorts and bikini tops.

“None of the hits that were received were relevant,” two Navy cryptologic technicians write in one of many summaries of nonproductive surveillance. “No additional information,” writes a civilian analyst. Another makes fun of a suspected kidnapper, newly arrived in Syria before the current civil war, who begs for employment as a janitor and makes wide-eyed observations about the state of undress displayed by women on local beaches.

By law, the NSA may “target” only foreign nationals located overseas unless it obtains a warrant based on probable cause from a special surveillance court. For collection under PRISM and Upstream rules, analysts must state a reasonable belief that the target has information of value about a foreign government, a terrorist organization or the spread of nonconventional weapons.

Most of the people caught up in those programs are not the targets and would not lawfully qualify as such. “Incidental collection” of third-party communications is inevitable in many forms of surveillance, but in other contexts the U.S. government works harder to limit and discard irrelevant data. In criminal wiretaps, for example, the FBI is supposed to stop listening to a call if a suspect’s wife or child is using the phone.

There are many ways to be swept up incidentally in surveillance aimed at a valid foreign target. Some of those in the Snowden archive were monitored because they interacted directly with a target, but others had more-tenuous links.

If a target entered an online chat room, the NSA collected the words and identities of every person who posted there, regardless of subject, as well as every person who simply “lurked,” reading passively what other people wrote.

“1 target, 38 others on there,” one analyst wrote. She collected data on them all.

In other cases, the NSA designated as its target the Internet protocol, or IP, address of a computer server used by hundreds of people.

The NSA treats all content intercepted incidentally from third parties as permissible to retain, store, search and distribute to its government customers. Raj De, the agency’s general counsel, has testified that the NSA does not generally attempt to remove irrelevant personal content, because it is difficult for one analyst to know what might become relevant to another.

The Obama administration declines to discuss the scale of incidental collection. The NSA, backed by Director of National Intelligence James R. Clapper Jr., has asserted that it is unable to make any estimate, even in classified form, of the number of Americans swept in. It is not obvious why the NSA could not offer at least a partial count, given that its analysts routinely pick out “U.S. persons” and mask their identities, in most cases, before distributing intelligence reports.

If Snowden's sample is representative, the population under scrutiny in the PRISM and Upstream programs is far larger than the government has suggested. In a June 26 "transparency report," the Office of the Director of National Intelligence disclosed that 89,138 people were targets of last year's collection under FISA Section 702. At the 9-to-1 ratio of incidental collection in Snowden's sample, the office's figure would correspond to nearly 900,000 accounts, targeted or not, under surveillance.

'He didn't get this data'

U.S. intelligence officials declined to confirm or deny in general terms the authenticity of the intercepted content provided by Snowden, but they made off-the-record requests to withhold specific details that they said would alert the targets of ongoing surveillance. Some officials, who declined to be quoted by name, described Snowden's handling of the sensitive files as reckless.

In an interview, Snowden said "primary documents" offered the only path to a concrete debate about the costs and benefits of Section 702 surveillance. He did not favor public release of the full archive, he said, but he did not think a reporter could understand the programs "without being able to review some of that surveillance, both the justified and unjustified."

"While people may disagree about where to draw the line on publication, I know that you and The Post have enough sense of civic duty to consult with the government to ensure that the reporting on and handling of this material causes no harm," he said.

In Snowden's view, the PRISM and Upstream programs have "crossed the line of proportionality."

"Even if one could conceivably justify the initial, inadvertent interception of baby pictures and love letters of innocent bystanders," he added, "their continued storage in government databases is both troubling and dangerous. Who knows how that information will be used in the future?"

For close to a year, NSA and other government officials have appeared to deny, in congressional testimony and public statements, that Snowden had any access to the material.

As recently as May, shortly after he retired as NSA director, Gen. Keith Alexander denied that Snowden could have passed FISA content to journalists.

"He didn't get this data," Alexander told a New Yorker reporter. "They didn't touch —"

"The operational data?" the reporter asked.

"They didn't touch the FISA data," Alexander replied. He added, "That database, he didn't have access to."

Robert S. Litt, the general counsel for the Office of the Director of National Intelligence, said in a prepared statement that Alexander and other officials were speaking only about "raw" intelligence, the term for intercepted content that has not yet

been evaluated, stamped with classification markings or minimized to mask U.S. identities.

“We have talked about the very strict controls on raw traffic, the training that people have to have, the technological lockdowns on access,” Litt said. “Nothing that you have given us indicates that Snowden was able to circumvent that in any way.”

In the interview, Snowden said he did not need to circumvent those controls, because his final position as a contractor for Booz Allen at the NSA’s Hawaii operations center gave him “unusually broad, unescorted access to raw SIGINT [signals intelligence] under a special ‘Dual Authorities’ role,” a reference to Section 702 for domestic collection and Executive Order 12333 for collection overseas. Those credentials, he said, allowed him to search stored content — and “task” new collection — without prior approval of his search terms.

“If I had wanted to pull a copy of a judge’s or a senator’s e-mail, all I had to do was enter that selector into XKEYSCORE,” one of the NSA’s main query systems, he said.

The NSA has released an e-mail exchange acknowledging that Snowden took the required training classes for access to those systems.

‘Minimized U.S. president’

At one level, the NSA shows scrupulous care in protecting the privacy of U.S. nationals and, by policy, those of its four closest intelligence allies — Britain, Australia, Canada and New Zealand.

More than 1,000 distinct “minimization” terms appear in the files, attempting to mask the identities of “possible,” “potential” and “probable” U.S. persons, along with the names of U.S. beverage companies, universities, fast-food chains and Web-mail hosts.

Some of them border on the absurd, using titles that could apply to only one man. A “minimized U.S. president-elect” begins to appear in the files in early 2009, and references to the current “minimized U.S. president” appear 1,227 times in the following four years.

Even so, unmasked identities remain in the NSA’s files, and the agency’s policy is to hold on to “incidentally” collected U.S. content, even if it does not appear to contain foreign intelligence.

In one exchange captured in the files, a young American asks a Pakistani friend in late 2009 what he thinks of the war in Afghanistan. The Pakistani replies that it is a religious struggle against 44 enemy states.

Startled, the American says “they, ah, they aren’t heavily participating . . . its like . . . in a football game, the other team is the enemy, not the other teams waterboy and cheerleaders.”

“No,” the Pakistani shoots back. “The ther teams water boy is also an enemy. it is law of our religion.”

“haha, sorry thats kind of funny,” the American replies.

When NSA and allied analysts really want to target an account, their concern for U.S. privacy diminishes. The rationales they use to judge foreignness sometimes stretch legal rules or well-known technical facts to the breaking point.

In their classified internal communications, colleagues and supervisors often remind the analysts that PRISM and Upstream collection have a “lower threshold for foreignness ‘standard of proof’ ” than a traditional surveillance warrant from a FISA judge, requiring only a “reasonable belief” and not probable cause.

One analyst rests her claim that a target is foreign on the fact that his e-mails are written in a foreign language, a quality shared by tens of millions of Americans. Others are allowed to presume that anyone on the chat “buddy list” of a known foreign national is also foreign.

In many other cases, analysts seek and obtain approval to treat an account as “foreign” if someone connects to it from a computer address that seems to be overseas. “The best foreignness explanations have the selector being accessed via a foreign IP address,” an NSA supervisor instructs an allied analyst in Australia.

Apart from the fact that tens of millions of Americans live and travel overseas, additional millions use simple tools called proxies to redirect their data traffic around the world, for business or pleasure. World Cup fans this month have been using a browser extension called Hola to watch live-streamed games that are unavailable from their own countries. The same trick is routinely used by Americans who want to watch BBC video. The NSA also relies routinely on locations embedded in Yahoo tracking cookies, which are widely regarded by online advertisers as unreliable.

In an ordinary FISA surveillance application, the judge grants a warrant and requires a fresh review of probable cause — and the content of collected surveillance — every 90 days. When renewal fails, NSA and allied analysts sometimes switch to the more lenient standards of PRISM and Upstream.

“These selectors were previously under FISA warrant but the warrants have expired,” one analyst writes, requesting that surveillance resume under the looser standards of Section 702. The request was granted.

‘I don’t like people knowing’

She was 29 and shattered by divorce, converting to Islam in search of comfort and love. He was three years younger, rugged and restless. His parents had fled Kabul and raised him in Australia, but he dreamed of returning to Afghanistan.

One day when she was sick in bed, he brought her tea. Their faith forbade what happened next, and later she recalled it with shame.

“what we did was evil and cursed and may allah swt MOST merciful forgive us for giving in to our nafs [desires]”

Still, a romance grew. They fought. They spoke of marriage. They fought again.

All of this was in the files because, around the same time, he went looking for the Taliban.

He found an e-mail address on its English-language Web site and wrote repeatedly, professing loyalty to the one true faith, offering to “come help my brothers” and join the fight against the unbelievers.

On May 30, 2012, without a word to her, he boarded a plane to begin a journey to Kandahar. He left word that he would not see her again.

If that had been the end of it, there would not be more than 800 pages of anguished correspondence between them in the archives of the NSA and its counterpart, the Australian Signals Directorate.

He had made himself a target. She was the collateral damage, placed under a microscope as she tried to adjust to the loss.

Three weeks after he landed in Kandahar, she found him on Facebook.

“Im putting all my pride aside just to say that i will miss you dearly and your the only person that i really allowed myself to get close to after losing my ex husband, my dad and my brother.. Im glad it was so easy for you to move on and put what we had aside and for me well Im just soo happy i met you. You will always remain in my heart. I know you left for a purpose it hurts like hell sometimes not because Im needy but because i wish i could have been with you.”

His replies were cool, then insulting, and gradually became demanding. He would marry her but there were conditions. She must submit to his will, move in with his parents and wait for him in Australia. She must hand him control of her Facebook account — he did not approve of the photos posted there.

She refused. He insisted:

“look in islam husband doesnt touch girl financial earnigs unless she agrees but as far as privacy goes there is no room....i need to have all ur details everything u do its what im supposed to know that will guide u whether its right or wrong got it”

Later, she came to understand the irony of her reply:

“I don’t like people knowing my private life.”

Months of negotiations followed, with each of them declaring an end to the romance a dozen times or more. He claimed he had found someone else and planned to marry that day, then admitted it was a lie. She responded:

“No more games. You come home. You won’t last with an afghan girl.”

She begged him to give up his dangerous path. Finally, in September, she broke off contact for good, informing him that she was engaged to another man.

“When you come back they will send you to jail,” she warned.

They almost did.

In interviews with The Post, conducted by telephone and Facebook, she said he flew home to Australia last summer, after failing to find members of the Taliban who would take him seriously. Australian National Police met him at the airport and questioned him in custody. They questioned her, too, politely, in her home. They showed her transcripts of their failed romance. When a Post reporter called, she already knew what the two governments had collected about her.

Eventually, she said, Australian authorities decided not to charge her failed suitor with a crime. Police spokeswoman Emilie Lovatt declined to comment on the case.

Looking back, the young woman said she understands why her intimate correspondence was recorded and parsed by men and women she did not know.

“Do I feel violated?” she asked. “Yes. I’m not against the fact that my privacy was violated in this instance, because he was stupid. He wasn’t thinking straight. I don’t agree with what he was doing.”

What she does not understand, she said, is why after all this time, with the case long closed and her own job with the Australian government secure, the NSA does not discard what it no longer needs.

Jennifer Jenkins and Carol D. Leonnig contributed to this report.

Barton Gellman writes for the national staff. He has contributed to three Pulitzer Prizes for The Washington Post, most recently the 2014 Pulitzer Prize for Public Service. [🐦 Follow @bartongellman](#)

Share news tips with us confidentially

Do you have information the public should know? Here are some ways you can securely send information and documents to Post journalists.

Learn more

Exhibit 8



MENU



US

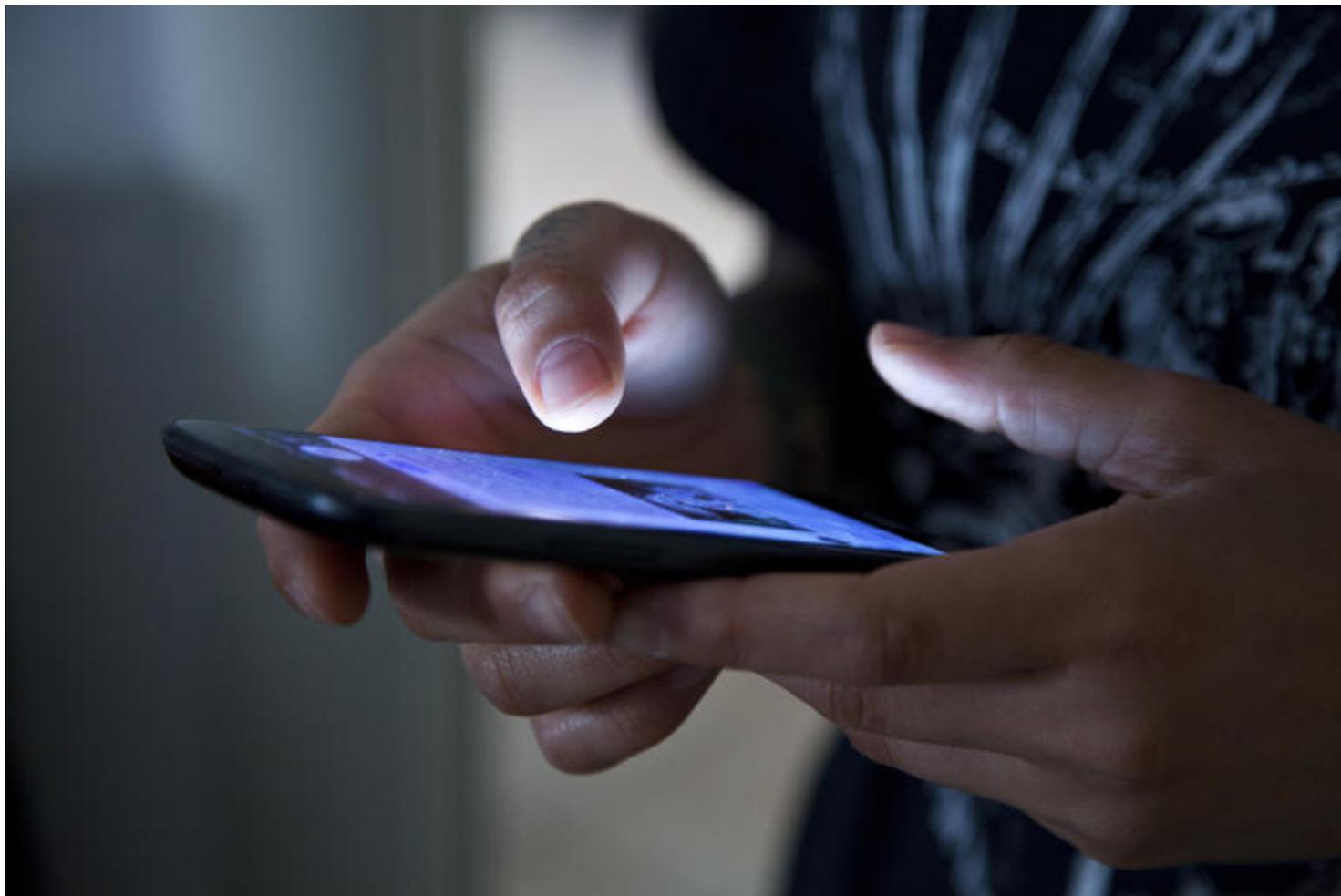
JUST IN **SPACEX BFR TO LEAD WAY TO MARS WHILE GOING ANYWHERE ON EARTH WITHIN AN HOUR**

With a single wiretap order, US authorities listened in on 3.3 million phone calls

The order was carried out in 2016 as part of a federal narcotics investigation.



By Zack Whittaker for Zero Day | June 30, 2017 -- 18:07 GMT (11:07 PDT) | Topic: Security



(Image: file photo)

NEW YORK, NY -- US authorities intercepted and recorded millions of phone calls last year under a single wiretap order, authorized as part of a narcotics investigation.

The wiretap order authorized an unknown government agency to carry out real-time intercepts of 3.29 million cell phone conversations over a two-month period at some point during 2016, after the order was applied for in late 2015.

The order was signed to help authorities track 26 individuals suspected of involvement with illegal drug and narcotic-related activities in Pennsylvania.

The wiretap cost the authorities \$335,000 to conduct and led to a dozen arrests.

But the authorities noted that the surveillance effort led to no incriminating intercepts, and none of the handful of those arrested have been brought to trial or convicted.

The revelation was buried in the US Courts' annual wiretap report, published [earlier this week](http://www.uscourts.gov/statistics-reports/wiretap-report-2016) (<http://www.uscourts.gov/statistics-reports/wiretap-report-2016>) but largely overlooked.

"The federal wiretap with the most intercepts occurred during a narcotics investigation in the Middle District of Pennsylvania and resulted in the interception of 3,292,385 cell phone conversations or messages over 60 days," said the report.

Details of the case remain largely unknown, likely in part because the wiretap order and several motions that have been filed in relation to the case are thought to be under seal.

It's understood to be one of the largest number of calls intercepted by a single wiretap in years, though it's not known the exact number of Americans whose communications were caught up by the order.

We contacted the US Attorney's Office for the Middle District of Pennsylvania, where the wiretap application was filed, but did not hear back.

Albert Gidari, a former privacy lawyer who now serves as director of privacy at Stanford Law School's Center for Internet and Society, criticized the investigation.

"They spent a fortune tracking 26 people and recording three million conversations and apparently got nothing," said Gidari. "I'd love to see the probable cause affidavit for that one and wonder what the court thought on its 10 day reviews when zip came in."

"I'm not surprised by the results because on average, a very very low percentage of conversations are incriminating, and a very very low percent results in conviction," he added.

When reached, a spokesperson for the Justice Department did not comment.

Contact me securely (<https://medium.com/@zackwhittaker/how-to-contact-me-securely-38dc5c5bc756>)

Zack Whittaker can be reached securely on Signal and WhatsApp at 646-755-8849, and his PGP fingerprint for email is: 4D0E 92F2 E36A EC51 DAAE 5D97 CB8C 15FA EB6C EEA5.

Read More (<https://medium.com/@zackwhittaker/how-to-contact-me-securely-38dc5c5bc756>)

ZDNET INVESTIGATIONS

Leaked TSA documents reveal New York airport's wave of security lapses (<http://www.zdnet.com/article/leaked-files-reveal-catalog-of-airport-security-lapses/>)

US government pushed tech firms to hand over source code (<http://www.zdnet.com/article/us-government-pushed-tech-firms-to-hand-over-source-code/>)

At the US border: Discriminated, detained, searched, interrogated (<http://www.zdnet.com/article/welcome-to-the-united-states-discriminated-detained-searched-interrogated-special-report/>)

Millions of Verizon customer records exposed in security lapse (<http://www.zdnet.com/article/millions-verizon-customer-records-israeli-data/>)

Meet the shadowy tech brokers that deliver your data to the NSA (<http://www.zdnet.com/article/meet-the-shadowy-tech-brokers-that-deliver-your-data-to-the-nsa/>)

Inside the global terror watchlist that secretly shadows millions (<http://www.zdnet.com/article/inside-the-global-terrorism-blacklist-secretly-shadowing-millions-of-suspects/>)

FCC chairman voted to sell your browsing history — so we asked to see his (<http://www.zdnet.com/article/fcc-chairman-browsing-history-freedom-of-information/>)

Exhibit 9

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide
FOR OFFICIAL USE ONLY



U.S. Department of Justice

National Security Division

Office of the Assistant Attorney General

Washington, D.C. 20530

January 10, 2008

TO: All United States Attorneys
All National Security Division Attorneys
All Anti-Terrorism Coordinators

CC: Assistant Attorney General, Criminal Division
Assistant Attorney General, Civil Division
Director, Federal Bureau of Investigation

FROM: Kenneth L. Wainstein *KLW*
Assistant Attorney General for National Security

SUBJECT: Revised FISA Use Policy as Approved by the Attorney General

We are pleased to provide the Department of Justice's revised policy on the use or disclosure of information obtained or derived from collections under the Foreign Intelligence Surveillance Act of 1978 (FISA), as approved by the Attorney General today. Also attached is a form for use with respect to notifications that are required under Section I of the revised policy.

This revised policy includes significant changes from current practice that will streamline the process for using FISA information in certain basic investigative processes, while still ensuring that important intelligence and law enforcement interests are protected.

You will note that the revised policy authorizes the use or disclosure of FISA information, under the specific circumstances described in the policy, with notification to NSD and after consultation with the FBI (or other Intelligence Community agencies) for the following investigative processes:



b7E

FOR OFFICIAL USE ONLY

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-01-2011 BY UC 60322 LP/PJ/SZ

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide
FOR OFFICIAL USE ONLY

b7E

- 
- 
- 

As described in the revised policy, the Department continues to require prior authorization from the Assistant Attorney General for National Security (AAG/NSD) for the use or disclosure of FISA information in order to file criminal charges or in post-charge criminal proceedings, as well as in connection with certain investigative processes (*e.g.*, criminal search warrants under Rule 41 of the Federal Rules of Criminal Procedure). The revised policy also requires the prior authorization of the AAG/NSD or his designee for the use or disclosure of FISA information in non-criminal proceedings.

The revised policy was drafted by a Justice Department working group that included representatives from the Attorney General's Advisory Committee of United States Attorneys (AGAC), National Security Division (NSD), Federal Bureau of Investigation (FBI), and Office of Legal Policy (OLP). The working group also consulted with the Office of the Director of National Intelligence (ODNI) in the course of the development of this policy.

The revised policy requires that it be reviewed one year from its effective date and requires NSD to issue guidance on what constitutes information "derived from" FISA collections by March 31, 2008.

As noted in the policy, prosecutors are encouraged to contact the National Security Division at any time in order to obtain guidance regarding this policy and to expedite resolution of any issues.

FOR OFFICIAL USE ONLY

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-01-2011 BY UC 60322 LP/PJ/SZ

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

FOR OFFICIAL USE ONLY



U.S. Department of Justice

Office of the Attorney General

Washington, D.C. 20530

January 10, 2008

TO: All Federal Prosecutors

CC: Assistant Attorney General, National Security Division
Assistant Attorney General, Criminal Division
Assistant Attorney General, Civil Division
Director, Federal Bureau of Investigation

FROM: Michael B. Mukasey 
Attorney General

SUBJECT: Revised Policy on the Use or Disclosure of FISA Information

As a general matter, it is the policy of the Department of Justice to use all lawful processes in the investigation and prosecution of cases involving terrorism, intelligence, and national security, and to undertake all efforts necessary to protect the American people from the threat posed by foreign powers and their agents, while also exercising due regard for the protection of intelligence sources, methods, and collections, and the privacy and civil liberties of United States persons.

There are important purposes to be served by consultation and coordination with respect to the use or disclosure of FISA information¹ in investigations, criminal prosecutions, and other proceedings. First, because FISA information is almost always classified, the use or disclosure of such information will normally require declassification by the originating agency in accordance with the originating agency's policies and procedures. Second, the use of such information could directly or indirectly compromise intelligence sources, methods, or collections, or disclose the existence or nature of or otherwise compromise an investigation. Third, FISA requires the Government to notify the court and an "aggrieved person" of its intent

¹ The term "FISA information," as used in this policy, means any information acquired, obtained, or derived from collection authorized pursuant to FISA. Whether specific information qualifies as "derived from" FISA collection may be a fact-bound question that depends, at least in part, on the attenuation of the information to be used from the original FISA acquired or obtained information and whether the information was also obtained from an independent source, as well as other factors. Where such a question arises, the application of this policy should be discussed among the USAO, FBI, and NSD, and if consensus is not reached, a determination will be made by the Assistant Attorney General for National Security. Separate guidance regarding what constitutes information "derived from" FISA collection will be issued by the National Security Division no later than March 31, 2008.

FOR OFFICIAL USE ONLY

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

FOR OFFICIAL USE ONLY

to use or disclose any FISA information before it is used against such person in a broad range of proceedings. Fourth, the Government is required to ensure that complete and accurate filings are made with the Foreign Intelligence Surveillance Court (FISC), and that the Government complies with all of FISA's statutory requirements. Fifth, it is important to ensure that litigation risks, if any, are properly assessed. Finally, in certain cases, it may be appropriate to make disclosures to a United States District Court regarding classified facts before legal process is obtained.

Given these purposes, it is essential that coordination take place in connection with the use or disclosure of FISA information. Such coordination should be streamlined in order to promote efficient, nimble, and useful investigative activities. The risk of compromising the purposes described above varies depending on the stage of the investigation, criminal prosecution, or other proceeding. As a general matter, [REDACTED] b7E

[REDACTED] federal prosecutors should consider alternative approaches for taking action.

Prosecutors are encouraged to contact the National Security Division at any time in order to obtain guidance regarding this policy and to expedite resolution of any issues.

The following policy is therefore adopted and supersedes any existing Attorney General policies with respect to the use and disclosure of FISA information to the extent that they are inconsistent with this policy:

- (a) the Assistant Attorney General for National Security may act as the Attorney General, as provided for under FISA, *see* 50 U.S.C. § 1801(g), for the purpose of authorizing the use or disclosure of FISA information pursuant to this policy;² and
- (b) federal prosecutors and all others who may seek to use or disclose FISA information in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, in coordination with NSD and FBI, are authorized to do so pursuant to the terms of this policy, shall coordinate with NSD [REDACTED] b7E
[REDACTED] and shall comply with the following procedures in matters that involve the use or disclosure of FISA information:³

² Such authorization may also be provided by the Attorney General, Acting Attorney General, and the Deputy Attorney General. *See* 50 U.S.C. § 1801(g).

³ Nothing in this policy is intended to supersede or replace existing policies for prosecutors regarding notification, consultation, and approval for certain investigative and prosecutive steps, including consultation with other districts where related matters may be under investigation. For example, the United States Attorneys' Manual sets forth when a prosecutor must obtain prior approval for various court actions in national security prosecutions. *See, e.g.,* United States Attorneys' Manual (USAM) §§ 9-2.131 ("Matters Assumed by Criminal Division or Higher

FOR OFFICIAL USE ONLY

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

FOR OFFICIAL USE ONLY

I. Use or Disclosure of FISA Information Requiring Consultation with FBI or other Intelligence Community Agencies and Notification to NSD

A. Certain investigative processes present only moderate risks. As a result, where FISA information is used or disclosed in connection with the processes described below, consultation with FBI (or other Intelligence Community agencies, as appropriate)⁴ and notice to NSD is required: b7E

- 1. [Redacted]
- 2. [Redacted]
- 3. [Redacted]
- 4. [Redacted]

B. Where FISA information is used or disclosed in connection with the processes described above, the following notification process shall be followed:

- 1. [Redacted]

Authority”); 9-2.136 (“Investigative and Prosecutive Policy for International Terrorism Matters”); 9-2.155 (“Sensitive Matters”); 9-2.400 (“Prior Approvals Chart”).

⁴ For the purposes of this document, the term “Intelligence Community agencies” refers to the appropriate agencies within the Intelligence Community, including the Office of the Director of National Intelligence. Consultation with Intelligence Community agencies other than the FBI is typically appropriate when the sources, methods, or collections involve Intelligence Community agencies other than the FBI. Prosecutors are encouraged to contact the National Security Division, as needed, to assist with the consultation process with the FBI or other Intelligence Community agencies.

⁵ Some courts require a significant measure of information with respect to [Redacted] b7E
[Redacted] To the extent that applications in such districts require the disclosure of additional FISA information beyond the disclosure of [Redacted]
[Redacted] advance authorization as provided for in Section II of this policy is required prior to such applications being made to the court.

FOR OFFICIAL USE ONLY

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

FOR OFFICIAL USE ONLY

b7E

- 2. As provided on the attached draft [redacted] the federal prosecutor must indicate that he or she has [redacted]

[redacted]

- 3. [redacted]

above—to ensure that NSD complies with potential obligations to notify the Foreign Intelligence Surveillance Court.

- C. Where consultations with the FBI (or other Intelligence Community agencies, as appropriate) demonstrate that [redacted]

[redacted]

further consultation that includes NSD (working with Intelligence Community agencies, as appropriate) shall take place prior to the use of such processes.

- 1. [redacted]

- D. This section does not permit the use or disclosure of FISA information obtained [redacted]

[redacted]

Federal prosecutors must seek specific, separate use authority from the Assistant Attorney General for National Security prior to initiating any criminal proceedings.

II. Use or Disclosure of FISA Information Requiring the Advance Authorization of the Assistant Attorney General for National Security

- A. The advance authorization of the Assistant Attorney General for National Security is required where FISA information is [redacted]

b7E

[redacted]

b7E

[redacted]

FOR OFFICIAL USE ONLY

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

FOR OFFICIAL USE ONLY

1. *Investigative Processes Requiring Advance Authorization*

a. [redacted] As a result, authorization of the Assistant Attorney General for National Security is required before FISA information is used or disclosed in connection with the processes described below:

b7E

i. [redacted]

ii. [redacted] Title 18, Chapter 119, United States Code;

iii. [redacted] Title 18, Chapter 121, United States Code;

iv. [redacted] Rule 41 of the Federal Rules of Criminal Procedure;

v. [redacted] 18 U.S.C. § 3144;

vi. [redacted]

vii. [redacted]

2. *Criminal Indictments and Post-Indictment Proceedings*

a. The use or disclosure of FISA information [redacted] As a result, the advance authorization of the Assistant Attorney General for National Security is required before such use or disclosure.

b7E

b. This advance authorization requirement applies to [redacted]

b7E

FOR OFFICIAL USE ONLY

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

FOR OFFICIAL USE ONLY

- 3. Among the factors that will be considered with respect to granting use authority are:

b7E

- 4. Because the process of obtaining advance authorization will require NSD to coordinate with Intelligence Community agencies, federal prosecutors should seek such advance authorization at the earliest juncture possible. In addition, because the use of such information will normally require

- a. Prosecutors are encouraged to contact NSD at any time in order to obtain guidance regarding this policy and to expedite resolution of any issues.

- b. Where advance authorization involving [redacted] [redacted] NSD shall provide notice of such request to ODNI.

III. Use or Disclosure of FISA Information In Non-Criminal Proceedings

- A. [redacted] Therefore, authorization of the Assistant Attorney General for National Security or his designee is required before such use or disclosure.

b7E

- 1. [redacted]

FOR OFFICIAL USE ONLY

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

FOR OFFICIAL USE ONLY

b7E

2. Among the factors that will be considered with respect to granting use authority are [REDACTED]

[REDACTED]

3. Because the process of obtaining advance authorization will require NSD to coordinate with Intelligence Community agencies, the attorney for the government should seek such advance authorization at the earliest juncture possible. In addition, because the use of such information will normally require [REDACTED]

[REDACTED]

- a. Prosecutors are encouraged to contact NSD at any time in order to obtain guidance regarding this policy and to expedite resolution of any issues.
 - b. Where advance authorization involving particularly sensitive sources, methods, or collections is requested, NSD shall provide notice of such request to ODNI.
- This policy shall be reviewed one year from its effective date to evaluate its effectiveness.

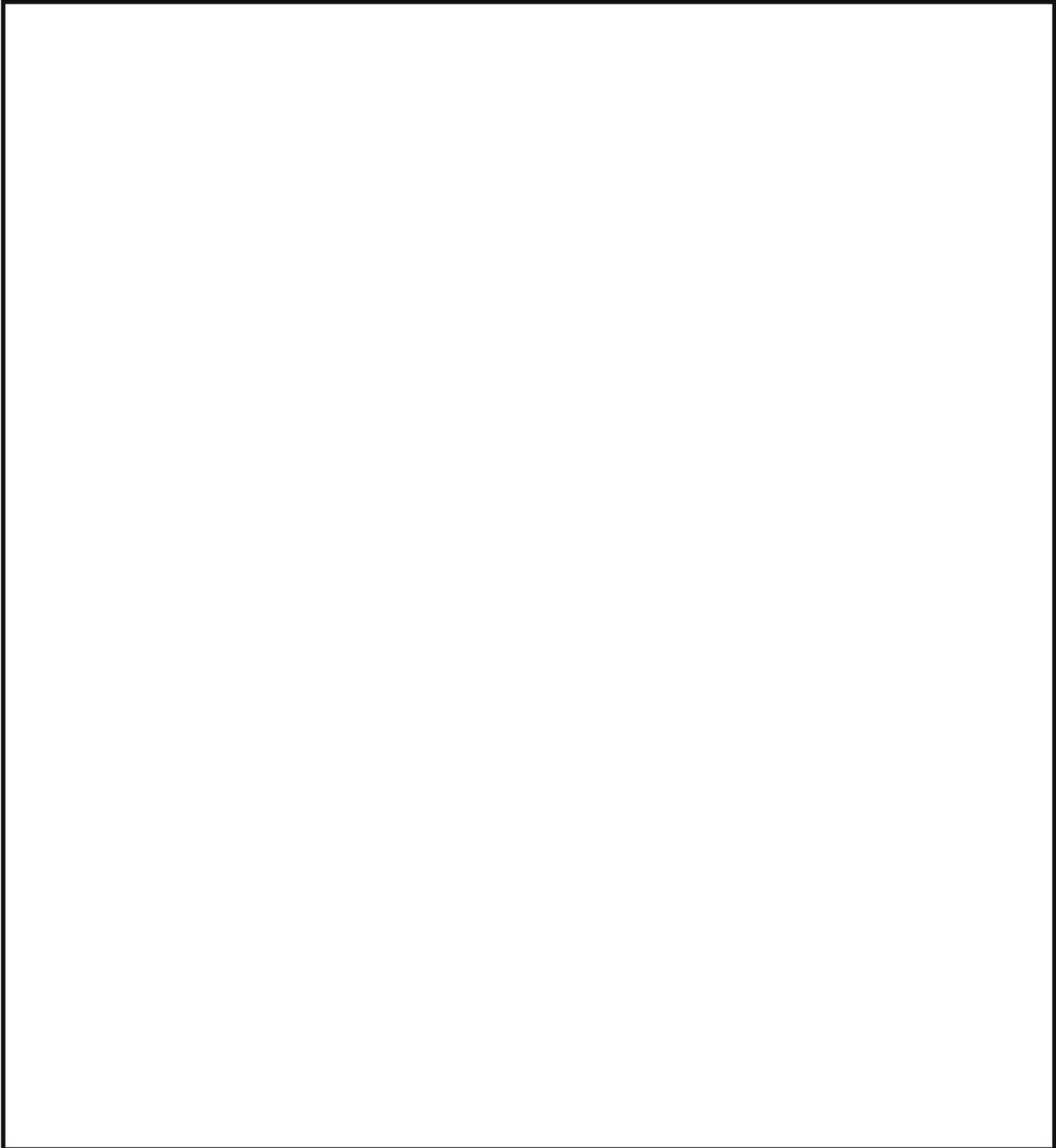
FOR OFFICIAL USE ONLY

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

Classification:

b5

NOTIFICATION OF USE OR DISCLOSURE OF FISA INFORMATION FORM



ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-01-2011 BY UC 60322 LP/PJ/SZ

Classification:

E-11
UNCLASSIFIED – FOR OFFICIAL USE ONLY

Version Dated:
October 15, 2011

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

b5

Classification:



Classification:

2

Exhibit 10

PREPARED STATEMENT OF DANIEL J. BRYANT

Good morning, Mr. Chairman and distinguished members of the Subcommittee. Thank you for the opportunity to appear before you today to discuss H.R. 3179, the Anti-Terrorism Intelligence Tools Improvement Act of 2003.

Since the brutal terrorist attacks of September 11, 2001, the Department of Justice has made significant strides in the war against terrorism. We have prosecuted many cases, among them being 310 individuals charged with criminal offenses as a result of terrorism investigations. 179 of these defendants already have been convicted. We have broken up terrorist cells in Buffalo, Charlotte, Portland, and northern Virginia. Due to interagency and international cooperation, nearly two-thirds of Al Qaeda's leadership worldwide has been captured or killed. And we are steadily dismantling the terrorists' financial network: around the world, \$136 million in assets have been frozen in 660 accounts.

[Page 18](#)

[PREV PAGE](#)

[TOP OF DOC](#)

These successes would not have been possible without the support of Congress in general and this Subcommittee in particular. On behalf of the Department, I would like to thank you for providing us with the tools and resources that have made it possible for the Department to effectively wage the war against terrorism.

As recent events in Madrid and Saudi Arabia remind us, however, our fight against terrorism is far from over. Our nation's terrorist enemies remain determined to visit death and destruction upon the United States and its allies, and we must maintain our vigilance and resolve in the face of this continuing threat. It is for this reason that the Department of Justice's top priority remains the prevention and disruption of terrorist attacks before they occur. Rather than waiting for terrorists to strike and then prosecuting those terrorists for their crimes, the Department seeks to identify and apprehend terrorists before they are able to carry out their nefarious plans.

The success of this prevention strategy depends, however, upon the Department's capacity to detect terrorist plots before they are executed. And the key to detecting such plots in a timely manner is the acquisition of information. Simply put, our ability to prevent terrorism is directly correlated with the quantity and quality of intelligence we are able to obtain and analyze.

Following the terrorist attacks of September 11, Congress provided the Department in the USA PATRIOT Act with a number of important tools that have enhanced our ability to gather information so that we may detect and disrupt terrorist plots. To give just one example, before the USA PATRIOT Act, law enforcement agents possessed the authority to conduct electronic surveillance—by petitioning a court for a wiretap order—in the investigation of many ordinary, non-terrorism crimes, such as drug crimes, mail fraud, and passport fraud. Investigators, however, did not possess that same authority when investigating many crimes that terrorists are likely to commit, such as chemical weapons offenses, the use of weapons of mass destruction, and violent acts of terrorism transcending national borders. This anomaly was corrected by section 201 of the PATRIOT Act, which now enables law enforcement to conduct electronic surveillance when investigating the full-range of terrorism crimes.

[Page 19](#)

[PREV PAGE](#)

[TOP OF DOC](#)

But while Congress and the Administration working together have made significant strides in improving the Department's capacity to gather the intelligence necessary to prevent terrorist attacks, there is still more that needs to be done. This is why I would like to thank Chairman Sensenbrenner and Chairman Goss for their leadership in introducing H.R. 3179, the Anti-Terrorism Intelligence Tools Improvement Act of 2003, and to thank this Subcommittee for holding a hearing on this important piece of legislation. The Department of Justice strongly supports H.R. 3179. The bill contains a number of significant reforms that would assist the Department's efforts to collect intelligence key to disrupting terrorist plots and better allow the Department to protect that information in criminal trials and immigration proceedings. In my testimony today, I will briefly

review the five substantive provisions contained in H.R. 3179 and explain why the Department believes that each one of them would assist our efforts in the war against terrorism.

To begin with, H.R. 3179 would amend the Foreign Intelligence Surveillance Act to allow for surveillance of so-called "lone wolf" international terrorists. Currently, the definition of "agent of a foreign power" found in FISA includes individuals with ties to groups that engage in international terrorism. It does not, however, reach unaffiliated individuals who engage in international terrorism. As a result, investigations of "lone wolf" terrorists are currently not authorized under FISA. Rather, such investigations must proceed under the stricter standards and shorter time periods for investigating ordinary crimes set forth in Title III of the Omnibus Crime Control and Safe Streets Act of 1968, potentially resulting in unnecessary and dangerous delays and greater administrative burdens.

Section 4 of H.R. 3179 would plug this dangerous gap in FISA's coverage by expanding the definition of "agent of a foreign power" to include a non-United States person who is engaged in international terrorism or preparing to engage in international terrorism, even if he or she is not known to be affiliated with an international terrorist group.

[Page 20](#)

[PREV PAGE](#)

[TOP OF DOC](#)

The Department believes that section 4 of H.R. 3179 would strengthen our ability to protect the American people against terrorism. A single foreign terrorist with a chemical, biological, or radiological weapon could inflict catastrophic damage on this country. Consequently, there is no reason why the Department should be able to conduct FISA surveillance only of foreign terrorists whom we know to be affiliated with international terrorist groups. In some cases, a foreign terrorist may, in fact, be a member of an international terrorist group, but the Department may not be able to establish this fact. In other cases, a foreign terrorist may be a genuine lone wolf. In either of these scenarios, however, it is vital that the Department be able to conduct the appropriate surveillance of such terrorists under FISA so that we are able to effectively and efficiently gather the information necessary to prevent these terrorists from endangering the lives of the American people.

Expanding FISA to reach an individual foreign terrorist is a modest but important expansion of the statute. To be sure, under current law, the Department must show under FISA that a foreign terrorist is a member of an international terrorist group. The House Committee Report on FISA, however, suggested that a "group" of terrorists covered by current law might be as small as two or three persons, and the interests that courts have found to support the constitutionality of FISA are unlikely to differ appreciably between a case involving a terrorist group of two or three persons and a case involving a single terrorist. In addition, it is important to stress that this proposal would not change the standard for conducting surveillance of any United States person but rather would apply only to foreign terrorists.

The Senate has already acted in a strong bipartisan fashion to amend FISA to cover lone wolf terrorists. Section 4 of H.R. 3179 was included in S. 113, which passed the Senate on May 8, 2003, by a vote of 90 to 4. The Department urges the House of Representatives to follow suit and also pass this important proposal in order to plug this dangerous gap in the scope of FISA's coverage to cover "lone wolf" terrorists.

[Page 21](#)

[PREV PAGE](#)

[TOP OF DOC](#)

H.R. 3179 also includes two important provisions related to the use of national security letter (NSLs). NSLs are used by the FBI to obtain relevant information from specified third-parties in authorized international terrorism or espionage investigations. NSLs are similar to administrative subpoenas but narrower in scope. While administrative subpoenas can be used to collect a wide array of information, NSLs apply more narrowly to telephone and electronic communication transactional records, financial records from financial institutions, and consumer information from consumer reporting agencies, as well as certain financial, consumer, and travel records for certain government employees who have access to classified information.

In order to safeguard the integrity of the sensitive terrorism and espionage investigations in which NSLs are used, the NSL statutes generally prohibit persons from disclosing that they received these requests for information. See, e.g., 12 U.S.C. §3414(a)(3); 12 U.S.C. §3414(a)(5)(D); 15 U.S.C. §1681u(d); 15 U.S.C. §1681v(c); 18 U.S.C. §2709(c); 50 U.S.C. §436(b). But these same statutes contain no explicit penalty for persons who unlawfully disclose that they have received an NSL. Section 2 of H.R. 3179 would remedy this defect by creating a new statutory provision imposing criminal liability on those who knowingly violate NSL non-disclosure requirements. This new offense would be a misdemeanor punishable by up to a year of imprisonment, but would carry a stiffer penalty of up to five years of imprisonment if the unlawful disclosure was committed with the intent to obstruct an investigation or judicial proceeding.

Oftentimes, the premature disclosure of an ongoing terrorism investigation can lead to a host of negative repercussions, including the destruction of evidence, the flight of suspected terrorists, and the frustration of efforts to identify additional terrorist conspirators. For these reasons, the FBI has forgone using NSLs in some investigations for fear that the recipients of those NSLs would compromise an investigation by disclosing the fact that they had been sent an NSL. To reduce these fears and thus allow for the gathering of additional important information in terrorism investigations, the Department supports the adoption of the appropriate criminal penalties set forth in H.R. 3179 to deter the recipients of NSLs from violating applicable nondisclosure requirements as well as the heightened penalties set forth in the legislation for cases in which disclosures are actually intended to obstruct an ongoing investigation.

[Page 22](#)

[PREV PAGE](#)

[TOP OF DOC](#)

In addition to setting forth an explicit criminal penalty for those violating NSL nondisclosure requirements, H.R. 3179 would also specify procedures for the Attorney General to seek judicial enforcement of NSLs. The NSL statutes currently make compliance with an FBI request for information mandatory. See, e.g., 12 U.S.C. §3414(a)(5)(A); 15 U.S.C. §1681u(a)-(b); 15 U.S.C. §1681v(c); 18 U.S.C. §2709(a); 50 U.S.C. §436(c). These statutes, however, do not specify any procedures for judicial enforcement if the recipient of an NSL refuses to comply with the FBI's request. Section 3 of H.R. 3179 would make explicit what Congress indicated implicitly by making compliance with NSLs mandatory: the Attorney General may seek judicial enforcement in cases where the recipient of an NSL refuses to comply with the FBI's request for information. The judicial enforcement provision contained in H.R. 3179 is similar to the existing judicial enforcement provision for administrative subpoenas under 18 U.S.C. §3486(c) and would help the Department to quickly and discretely obtain vital information in terrorism investigations.

H.R. 3179 also includes two common-sense reforms that would better allow the Department to protect classified information in criminal trials and to safeguard sensitive intelligence investigations in immigration proceedings. First, section 5 of the bill would amend the Classified Information Procedures Act (CIPA) to improve the Department's ability to protect classified information during the course of a criminal trial. Under section 4 of CIPA, a district court, upon the government's request, may authorize the United States to delete specified items of classified information from documents to be made available to a criminal defendant during discovery, to substitute a summary of the information for such classified documents, or to submit a statement admitting relevant facts that the classified information would tend to prove, so long as prosecutors are able to make a sufficient showing, such as that the documents are not discoverable or that the defendant would not be disadvantaged by the substitution of a summary of the information for the classified documents themselves. Currently, however, district courts have discretion over whether to permit the government to make such a request ex parte and in camera.

[Page 23](#)

[PREV PAGE](#)

[TOP OF DOC](#)

This is problematic because in cases where the government is unable to make a request to withhold classified information ex parte and in camera, prosecutors risk disclosing sensitive national-security information simply by explaining in open court why the classified information in question should be protected. Section 5 of H.R. 3179 would solve this dilemma by mandating that prosecutors be able to make a request ex parte and in camera to

delete specified items of classified information from documents or to utilize the other alternatives for protecting classified information set forth in section 4 of CIPA. This provision would ensure that the Department is able to take appropriate steps to safeguard classified information in criminal proceedings without risking the disclosure of the very secrets that we are seeking to protect. It would also allow the Department to make a request to protect classified information orally as well as in writing.

In addition to understanding what this provision would accomplish, it is equally important to understand what this provision would not accomplish. Specifically, it would not affect in any way whatsoever the showing that the United States is required to make under section 4 of CIPA to obtain judicial authorization to withhold classified information from criminal defendants or to take other steps to safeguard classified information. Simply put, the assertion by some that H.R. 3179 would require a federal judge to permit the United States to turn over to a criminal defendant only a summary of evidence rather than classified documents themselves is demonstrably false. Rather, the bill would only allow the United States to make such a request *ex parte* and *in camera* in order to ensure that such information is not disclosed as part of the process of protecting it.

Finally, H.R. 3179 would eliminate that requirement that the United States notify aliens whenever the government intends to use evidence obtained through FISA in immigration proceedings. Current law mandates that the government provide notice to an "aggrieved person" if information obtained through FISA electronic surveillance, physical searches, or pen registers will be used in any federal proceeding. See 50 U.S.C. §1806(c), 1825(d), & 1845(c). In 1996, Congress carved out an exception to this requirement for alien terrorist removal proceedings, see 8 U.S.C. §1534(e), but all other immigration proceedings remain subject to this notification requirement.

[Page 24](#)

[PREV PAGE](#)

[TOP OF DOC](#)

Unfortunately, however, this mandate that the government notify an alien that it is using information acquired through FISA surveillance in an immigration proceeding may jeopardize in certain situations sensitive ongoing investigations and thus risk undermining national security. As a result, the government is sometimes faced with the Hobson's choice of not using this information in immigration proceedings, and possibly permitting dangerous aliens to remain in the country, or using the information and undermining its surveillance efforts. When faced with this difficult choice, the United States has decided against using FISA information in a number of instances in an effort to preserve the integrity of ongoing investigations.

Section 6 of H.R. 3179, however, would solve this dilemma by expanding the existing notification exception for alien terrorist removal proceedings to all immigration proceedings. Significantly, the government still would be obliged to disclose to aliens any information it intends to use in immigration proceedings if such disclosure is otherwise required by law. Under H.R. 3179, the government simply would not have to reveal the fact that the information in question was obtained through FISA. The Department supports this provision of H.R. 3179 because it would allow the government to use intelligence in immigration proceedings to safeguard the American people from dangerous aliens without jeopardizing sensitive ongoing investigations.

In conclusion, I would like to thank the Subcommittee again for holding today's hearing on such an important topic. H.R. 3179 contains a series of sensible reforms that would enhance the Department's ability to gather intelligence necessary for preventing terrorism and to protect the integrity of sensitive intelligence investigations. The Department would be happy to work with the Congress in the weeks and months to come on this vital piece of legislation. Thank you once again for allowing me to appear before you today, and I look forward to the opportunity to respond to any questions that you might have.

[Page 25](#)

[PREV PAGE](#)

[TOP OF DOC](#)

Exhibit 11

U.S.

Debate Brews Over Disclosing Warrantless Spying

By CHARLIE SAVAGE SEPT. 30, 2014

WASHINGTON — Obama administration lawyers have been debating whether the Treasury Department must inform the people or groups it lists as foreign terrorists when it relies on warrantless surveillance as the basis for the designation, according to officials familiar with the deliberations.

Intelligence officials are said to oppose being more forthcoming about who has been subjected to surveillance, especially in cases involving noncitizens abroad — who do not have Fourth Amendment privacy rights — because such information would tip them off that the National Security Agency had intercepted their communications.

But a provision in the Foreign Intelligence Surveillance Act, or FISA, requires the government to disclose when it uses information from eavesdropping in any “proceeding” against people. In 2008, Congress made the N.S.A.’s warrantless surveillance program a part of FISA, but the full implications of applying its disclosure provision to that program were overlooked.

Outside specialists said the same part of the law may apply to other government decisions that relied on such intelligence, including adding names to the “no fly” list and deciding whether to approve visas and licenses that require a security screening.

“This has so many potential spillovers that it’s fascinating,” said Robert M. Chesney, a law professor at the University of Texas at Austin.

The government began to scrutinize how the disclosure provision applied to the warrantless surveillance program in the summer of 2013, when leaks from Edward J. Snowden, the former N.S.A. contractor, were shining a spotlight on surveillance-related policies.

The scrutiny began in the Justice Department, where it became clear that prosecutors in the National Security Division had been concealing from criminal defendants — Americans protected by the Fourth Amendment — that some of the evidence they faced had been derived from warrantless wiretapping.

In August 2013, the department changed that practice and began notifying criminal defendants. Some of them have since challenged the program’s constitutionality, so far without success, though the litigation is in its early stages.

The ripples have spread to the Treasury Department, whose Office of Foreign Assets Control administers and enforces sanctions against people or groups that it designates as foreign terrorists, drug lords or other wrongdoers. Any American-based assets of those designated entities are frozen, and Americans may not do business with them.

Over the summer, lawyers for the Treasury Department had discussions with the National Security Division about whether — or at what stage — that process should count as a “proceeding” that falls under the disclosure provision, according to officials who spoke on the condition of anonymity to discuss internal deliberations.

When designating groups for sanctions, the Treasury Department announces its decision without notice. The designated groups can request that it reconsider; if that effort fails, they can file a lawsuit. Neither the designated groups nor their lawyers get to see any classified evidence against them, but at the lawsuit stage a judge is shown that information.

Erich C. Ferrari, a lawyer who represents foreign clients who have challenged their designations by the Treasury Department, said the government typically

provided very little information about the basis for its decisions. He argued that “the language of the statute should control” its interpretation and said he considered even the administrative reconsideration stage to be a “proceeding.” He added, “I think they would try to find a way to get out of that.”

Jimmy Gurule, a Notre Dame law professor who served from 2001 to 2003 as the Treasury Department’s under secretary for enforcement, a post that oversees the Office of Foreign Assets Control, said there was a strong argument that every stage of the process be counted as a “proceeding” because the statute was written broadly, meaning that the FISA notice law should apply from the start.

There is also precedent for the Treasury Department’s providing notice after a group has received its designation and is trying to have it reconsidered. In 2007, after an Ohio-based charity accused of funding Hamas asked to have its assets unfrozen, Treasury told the group that it was relying on FISA evidence for its designation, court papers show. But that case involved a FISA warrant targeting an entity on American soil.

The Treasury Department declined to explain how it has decided to interpret its obligations under the disclosure rule, although it provided a general statement.

“The Office of Foreign Assets Control is committed to complying fully with FISA, which we implement in close consultation and collaboration with the Department of Justice,” it said. “We are confident in the legality and validity of our designation actions, including decisions taken in response to delisting requests.”

The Obama administration has apparently decided that it does not need to ask Congress to change the FISA notice law. Several aides on the Intelligence and Judiciary Committees said the executive branch had not asked for modifications.

But the administration may also have decided to construe the notice law narrowly. Several precedents support the view that the FISA disclosure rule may not apply to the Treasury Department’s administrative process.

For example, courts have held in several cases involving regular law enforcement wiretaps — which have a similar notice rule — that only an adversarial

process, in which two sides present opposing views before a decision maker, counts as a covered “proceeding.” A court has also ruled that disclosure is not required when FISA information is shown to a grand jury.

Legal specialists said the government could also be invoking arguments against providing a FISA notice even at the court stage, which is adversarial. It may say, for example, that Congress could not have intended the law to apply in situations where the recipients of the notice could not do anything with that information. For example, most foreigners abroad could not argue that the warrantless surveillance violated their rights — because the Constitution does not cover them — and so they could not ask to have the evidence suppressed.

Still, the experts said surveillance-derived information could affect Americans who did have constitutional rights, like the approximately 800 people placed on the “no fly” list, which prevents people from boarding aircraft, as well as applicants for licenses like those that allow people to work behind airport security checkpoints.

“Very significant decisions about people’s lives are made on this kind of evidence,” said Jameel Jaffer, an American Civil Liberties Union lawyer. “When all this takes place in secret, you don’t have an opportunity to challenge the constitutionality of the government’s surveillance methods.”

In June, a Federal District Court judge struck down the process for challenging being put on the “no fly” list, saying it was too opaque and violated Americans’ due-process rights. She ordered the government to give people more information about why they are on the list.

A version of this article appears in print on October 1, 2014, on Page A3 of the New York edition with the headline: Debate Brews Over Disclosing Warrantless Spying.

Exhibit 12

the United States may oppose access to the classified information.

“(2) If, after consideration of any objection raised by the United States, including any objection asserted on the basis of privilege, the court determines that the defendant is legally entitled to have access to the information specified in the notice required by paragraph (1), the United States may request the substitution of a summary of the classified information or the substitution of a statement admitting relevant facts that the classified information would tend to prove.

“(3) The court shall permit the United States to make its objection to access or its request for such substitution in the form of a statement to be made ex parte and to be considered by the court alone. The entire text of the statement of the United States, as well as any summary of the classified information the defendant seeks to obtain, shall be sealed and preserved in the records of the court and made available to the appellate court in the event of an appeal.

“(4) The court shall grant the request of the United States to substitute a summary of the classified information or to substitute a statement admitting relevant facts that the classified information would tend to prove if it finds that the summary or statement will provide the defendant with substantially the same ability to make his defense as would disclosure of the specific classified information.

“(5) A defendant may not obtain access to classified information subject to this subsection except as provided in this subsection. Any proceeding, whether by deposition under the Federal Rules of Criminal Procedure or otherwise, in which a defendant seeks to obtain access to such classified information not previously authorized by a court for disclosure under this subsection must be discontinued or may proceed only as to lines of inquiry not involving such classified information.”

SA 3922. Mr. KYL submitted an amendment intended to be proposed by him to the bill S. 2248, to amend the Foreign Intelligence Surveillance Act of 1978, to modernize and streamline the provisions of that Act, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ____ . INVESTIGATION OF TERRORIST CRIMES.

(a) **NONDISCLOSURE OF FISA INVESTIGATIONS.**—The following provisions of the Foreign Intelligence Surveillance Act of 1978 are each amended by inserting “(other than in proceedings or other civil matters under the immigration laws, as that term is defined in section 101(a)(17) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(17))” after “authority of the United States”:

(1) Subsections (c), (e), and (f) of section 106 (50 U.S.C. 1806).

(2) Subsections (d), (f), and (g) of section 305 (50 U.S.C. 1825).

(3) Subsections (c), (e), and (f) of section 405 (50 U.S.C. 1845).

(b) **MULTIDISTRICT SEARCH WARRANTS IN TERRORISM INVESTIGATIONS.**—Rule 41(b)(3) of the Federal Rules of Criminal Procedure is amended to read as follows:

“(3) a magistrate judge—in an investigation of—

“(A) a Federal crime of terrorism (as defined in section 2332b(g)(g) of title 18, United States Code); or

“(B) an offense under section 1001 or 1505 of title 18, United States Code, relating to information or purported information con-

cerning a Federal crime of terrorism (as defined in section 2332b(g)(5) of title 18, United States Code)—having authority in any district in which activities related to the Federal crime of terrorism or offense may have occurred, may issue a warrant for a person or property within or outside that district.”.

(c) **INCREASED PENALTIES FOR OBSTRUCTION OF JUSTICE IN TERRORISM CASES.**—Sections 1001(a) and 1505 of title 18, United States Code, are amended by striking “8 years” and inserting “10 years”.

SA 3923. Mr. KYL submitted an amendment intended to be proposed by him to the bill S. 2248, to amend the Foreign Intelligence Surveillance Act of 1978, to modernize and streamline the provisions of that Act, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ____ . DENIAL OF FEDERAL BENEFITS TO CONVICTED TERRORISTS.

(a) **IN GENERAL.**—Chapter 113B of title 18, United States Code, is amended by adding at the end the following:

“§ 2339E. Denial of Federal benefits to terrorists

“(a) **IN GENERAL.**—Any individual who is convicted of a Federal crime of terrorism (as defined in section 2332b(g)) shall, as provided by the court on motion of the Government, be ineligible for any or all Federal benefits for any term of years or for life.

“(b) **FEDERAL BENEFIT DEFINED.**—In this section, ‘Federal benefit’ has the meaning given that term in section 421(d) of the Controlled Substances Act (21 U.S.C. 862(d)).”.

(b) **TABLE OF SECTIONS.**—The table of sections for chapter 113B of title 18, United States Code, is amended by adding at the end the following:

“2339D. Receiving military-type training from a foreign terrorist organization.

“2339E. Denial of Federal benefits to terrorists.”.

SA 3924. Mr. KYL submitted an amendment intended to be proposed by him to the bill S. 2248, to amend the Foreign Intelligence Surveillance Act of 1978, to modernize and streamline the provisions of that Act, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ____ . TERRORIST MURDERS, KIDNAPPINGS, AND ASSAULTS.

(a) **PENALTIES FOR TERRORIST MURDER AND MANSLAUGHTER.**—Section 2332(a) of title 18, United States Code, is amended—

(1) in paragraph (1), by striking “, punished by death” and all that follows and inserting “and punished by death or imprisoned for life;”;

(2) in paragraph (2), by striking “ten years” and inserting “30 years”.

(b) **ADDITION OF OFFENSE OF TERRORIST KIDNAPPING.**—Section 2332 of title 18, United States Code, is amended—

(1) by redesignating subsections (c) and (d) as subsections (d) and (e), respectively; and

(2) by inserting after subsection (b) the following:

“(c) **KIDNAPPING.**—Whoever outside the United States unlawfully seizes, confines, inveigles, decoys, kidnaps, abducts, or carries away, or attempts or conspires to seize, confine, inveigle, decoy, kidnap, abduct or carry away, a national of the United States shall

be fined under this title and imprisoned for any term of years or for life.”.

(c) **ADDITION OF SEXUAL ASSAULT TO DEFINITION OF OFFENSE OF TERRORIST ASSAULT.**—Section 2332(d) of title 18, United States Code, as redesignated by subsection (b) of this section, is amended—

(1) in paragraph (1), by inserting “(as defined in section 1365, including any conduct that, if the conduct occurred in the special maritime and territorial jurisdiction of the United States, would violate section 2241 or 2242)” after “injury”;

(2) in paragraph (2), by inserting “(as defined in section 1365, including any conduct that, if the conduct occurred in the special maritime and territorial jurisdiction of the United States, would violate section 2241 or 2242)” after “injury”; and

(3) in the matter following paragraph (2), by striking “or imprisoned” and all that follows and inserting “and imprisoned for any term of years not less than 30 or for life.”.

SA 3925. Mr. KYL submitted an amendment intended to be proposed by him to the bill S. 2248, to amend the Foreign Intelligence Surveillance Act of 1978, to modernize and streamline the provisions of that Act, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ____ . PREVENTION AND DETERRENCE OF TERRORIST SUICIDE BOMBINGS.

(a) **OFFENSE OF REWARDING OR FACILITATING INTERNATIONAL TERRORIST ACTS.**—

(1) **IN GENERAL.**—Chapter 113B of title 18, United States Code, is amended by adding at the end the following:

“§ 2339E. Providing material support to international terrorism

“(a) **DEFINITIONS.**—In this section:

“(1) The term ‘facility of interstate or foreign commerce’ has the same meaning as in section 1958(b)(2).

“(2) The term ‘international terrorism’ has the same meaning as in section 2331.

“(3) The term ‘material support or resources’ has the same meaning as in section 2339A(b).

“(4) The term ‘perpetrator of an act’ includes any person who—

“(A) commits the act;

“(B) aids, abets, counsels, commands, induces, or procures its commission; or

“(C) attempts, plots, or conspires to commit the act.

“(5) The term ‘serious bodily injury’ has the same meaning as in section 1365.

“(b) **PROHIBITION.**—Whoever, in a circumstance described in subsection (c), provides, or attempts or conspires to provide, material support or resources to the perpetrator of an act of international terrorism, or to a family member or other person associated with such perpetrator, with the intent to facilitate, reward, or encourage that act or other acts of international terrorism, shall be fined under this title, imprisoned for any term of years or for life, or both, and, if death results, shall be imprisoned for any term of years not less than 10 or for life.

(c) **JURISDICTIONAL BASES.**—A circumstance referred to in subsection (b) is that—

“(1) the offense occurs in or affects interstate or foreign commerce;

“(2) the offense involves the use of the mails or a facility of interstate or foreign commerce;

“(3) an offender intends to facilitate, reward, or encourage an act of international terrorism that affects interstate or foreign commerce or would have affected interstate

Exhibit 13

**APPLICABILITY OF THE FOREIGN INTELLIGENCE SURVEILLANCE
ACT'S NOTIFICATION PROVISION TO SECURITY CLEARANCE
ADJUDICATIONS BY THE DEPARTMENT OF JUSTICE
ACCESS REVIEW COMMITTEE**

The notification requirement in section 106(c) of the Foreign Intelligence Surveillance Act generally applies when the Department of Justice intends to use information obtained from electronic surveillance against an aggrieved person in an adjudication before the Access Review Committee concerning the Department's revocation of an employee's security clearance.

Compliance with the notification requirement in section 106(c) of the Foreign Intelligence Surveillance Act in particular Access Review Committee adjudications could raise as-applied constitutional questions if such notice would require disclosure of sensitive national security information protected by executive privilege.

June 3, 2011

**MEMORANDUM OPINION FOR THE CHAIR AND
MEMBERS OF THE ACCESS REVIEW COMMITTEE**

Section 106(c) of the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1806(c) (2006), requires the Government to notify an "aggrieved person"—that is, a person who was the target of electronic surveillance or whose communications or activities were subject to electronic surveillance, *see id.* § 1801(k)—whenever the Government intends to use "against" that person any information "obtained or derived from [such] electronic surveillance of that aggrieved person" in any "trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States." You have asked whether this notification requirement applies when the Department of Justice intends to use information obtained from such electronic surveillance against an aggrieved person in an adjudication before the Access Review Committee ("ARC") concerning the Department's revocation of an employee's security clearance.¹ In accord with views we received from the Department's Justice Management and National Security Divisions, we conclude that the notification requirement generally applies to such adjudications.² But, as we explain below, compliance with the notification requirement in particular ARC adjudications could raise as-

¹ See Memorandum for David Barron, Acting Assistant Attorney General, Office of Legal Counsel, from Mari Barr Santangelo, Chair, Access Review Committee, et al., *Re: Request for Opinion* (Jan. 26, 2010) ("*Request for Opinion*").

² See E-mail for Daniel L. Koffsky, Deputy Assistant Attorney General, Office of Legal Counsel, from Stuart Frisch, General Counsel, Justice Management Division, *Re: ARC request* (Apr. 2, 2010); E-mail for Daniel L. Koffsky, Deputy Assistant Attorney General, Office of Legal Counsel, from Todd Hinnen, Deputy Assistant Attorney General for Law and Policy, National Security Division, *Re: NSD Views Regarding the Applicability of 1806's Notification Provision to Access Review Committee Proceedings* (Mar. 31, 2010). We also received views from the Federal Bureau of Investigation ("FBI") that did not take issue with the position that section 106(c) applies to ARC adjudications, but that raised other, related issues, two of which we respond to below in note 3 and at pages 7-8. See Memorandum for the Acting Assistant Attorney General, Office of Legal Counsel, from Valerie Caproni, General Counsel, Federal Bureau of Investigation, *Re: Request for an OLC Opinion Dated January 26, 2010 by ARC* (Aug. 9, 2010) ("Caproni Memo").

Opinions of the Office of Legal Counsel in Volume 35

applied constitutional questions if such notice would require disclosure of sensitive national security information protected by executive privilege.

I.

Section 106(c) of FISA provides:

Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.

50 U.S.C. § 1806(c). Section 106(e), in turn, provides that the aggrieved person “may move to suppress the evidence obtained or derived from such electronic surveillance on the grounds that—(1) the information was unlawfully acquired; or (2) the surveillance was not made in conformity with an order of authorization or approval.” *Id.* § 1806(e).

You have asked us to assume, for purposes of our analysis, that a Department component has revoked an employee’s security clearance; that the loss of security clearance caused the component to discharge the employee; that the employee has appealed the component’s security-clearance revocation decision to the ARC; and that, in the course of the ARC adjudication, the Department intends to justify the clearance revocation with the use of information it has “obtained . . . from an electronic surveillance” of communications that involved the employee.³ *Id.* § 1806(c). Accordingly, we will assume that the employee in question would be an “aggrieved person” under section 106(c),⁴ and that the Government would use “information obtained . . . from an electronic surveillance of” that aggrieved person “against” that person in the ARC adjudication. *Id.*

The function of a security clearance for a Department employee is to designate the employee as someone who is eligible to be afforded access to classified information, in accordance with the standards set forth in part 3 of Executive Order 12968, 3 C.F.R. 391, 397

³ Because the circumstances you posit involve the use of information obtained directly from the electronic surveillance in question, we need not address the language in section 106(c) that also makes the section applicable when information has been “derived from” electronic surveillance.

⁴ Section 101(k) of FISA defines an “aggrieved person” as a “person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance.” 50 U.S.C. § 1801(k). In other words, “aggrieved person[s]” include only those persons targeted by the surveillance and others who are parties to communications subject to surveillance; as explained in a FISA House Report, “[t]he term specifically does not include persons, not parties to a communication, who may be mentioned or talked about by others.” H.R. Rep. No. 95-1283, pt. I, at 66 (1978).

Applicability of FISA's Notification Provision to Security Clearance Adjudications

(1996). *See* 28 C.F.R. § 17.41(a)(1) (2010). Executive Order 12968 provides in relevant part that eligibility for access to classified materials may be granted only to those employees

for whom an appropriate investigation has been completed and whose personal and professional history affirmatively indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information.

Exec. Order No. 12968, § 3.1(b), 3 C.F.R. at 397. The Executive Order requires that departments and agencies reinvestigate employees on a periodic basis, and it authorizes additional reinvestigation “if, at any time, there is reason to believe” that an employee “may no longer meet the standards for access established” by the Order. *Id.* § 3.4(b), 3 C.F.R. at 399.⁵ The applicable Department of Justice regulations accordingly provide that “[e]ligibility shall be granted only where facts and circumstances indicate access to classified information is clearly consistent with the national security interests of the United States and any doubt shall be resolved in favor of the national security.” 28 C.F.R. § 17.41(b).⁶

If a Department component denies an employee a security clearance—that is, if the component determines that the employee is not eligible for access to classified information—or if the component revokes such eligibility, the component must provide the employee “with a comprehensive and detailed written explanation of the basis” for the decision, to the extent that “the national security interests of the United States and other applicable law permit.” *Id.* § 17.47(a)(1). The component must also inform the employee that she has a right, at her own expense, to be represented by counsel or another representative of her choice. *Id.* During the thirty days following the date of the component’s written explanation of the clearance denial, the employee may request any “documents, records or reports” from the security clearance investigation, “including the entire investigative file upon which [the] denial or revocation [was] based,” *id.* § 17.47(a)(2), and within thirty days of such a request the employee must receive copies of the requested materials to the extent such materials would have been provided if requested under the Freedom of Information Act or the Privacy Act and “as the national security interests and other applicable law permit.” *Id.* § 17.47(a)(3). Thirty days after receiving the written explanation of the denial or the requested documents under § 17.47(a)(3)—whichever is later—the employee may file a written reply and request a review of the adverse determination.

⁵ In 2008, section 3(b) of Executive Order 13467 amended Executive Order 12968 in several respects, including by adding a new section 3.5 that provides for “continuous evaluation” of individuals determined to be eligible for access to classified information. *See* 3 C.F.R. §§ 196, 201 (2009). None of the 2008 amendments is germane to our analysis here.

⁶ *Eligibility* for access to classified information—i.e., having a security clearance—does not mean that an employee will necessarily be afforded access to such information. Both Executive Order 12968 and the Department’s regulations provide that eligibility for access is merely one prerequisite to actual access. In particular, an employee may not be provided access to such information without a demonstrated “need-to-know,” *see* Exec. Order No. 12968, § 1.2(a) & (c)(2), 3 C.F.R. at 392; 28 C.F.R. § 17.41(a)(2), and agencies must “ensure that access to classified information by each employee is clearly consistent with the interests of the national security,” Exec. Order No. 12968, § 1.2(b), 3 C.F.R. at 392; *accord* 28 C.F.R. § 17.41(c).

Opinions of the Office of Legal Counsel in Volume 35

Id. § 17.47(b). Thereafter, the employee must be provided a written notice of the results of the requested review, including the reasons for the results, along with the identity of the deciding authority and notice of the right to appeal an adverse decision to the ARC. The employee then may, within thirty days of receiving that written notice, appeal an adverse decision to the ARC and may request the opportunity to appear personally before the ARC and to present relevant documents, materials, and information. *Id.* § 17.47(d). The Department Security Officer must also be afforded an opportunity to present relevant materials to the ARC in support of the security clearance denial or revocation, and may appear personally if the employee does so. *Id.* § 17.47(g).

The ARC is composed of the Deputy Attorney General, the Assistant Attorney General for National Security, and the Assistant Attorney General for Administration—each of whom may name a designee, subject to the Attorney General’s approval. *See* 28 C.F.R. § 17.15(b). When an employee appeals an adverse security clearance decision, the ARC must make a written “determination of eligibility for access to classified information . . . as expeditiously as possible.” *Id.* § 17.47(f). Although the regulations describe this determination as a “discretionary security decision” by the ARC, they also mirror the regulations governing the component’s initial decision by providing that the ARC may conclude that an employee should be granted eligibility for access to classified materials “only where facts and circumstances indicate that access to classified information is clearly consistent with the national security interest of the United States”; any doubt is to be “resolved in favor of the national security.” *Id.* The ARC’s decision is final unless the Attorney General requests a recommendation from the ARC and “personally exercises appeal authority.” *Id.* § 17.15(a).

II.

Because the ARC is composed of three high-ranking Department officials or their designees and its decisions are final unless the Attorney General personally exercises appeal authority over them, an ARC adjudication challenging revocation of a security clearance takes place before a “department, officer[s], . . . or other authority of the United States.” 50 U.S.C. § 1806(c); *see* 28 U.S.C. § 501 (2006) (“[t]he Department of Justice is an executive department of the United States”); *see also* *Dong v. Smithsonian Inst.*, 125 F.3d 877, 881 (D.C. Cir. 1997) (“At the very least . . . it seems logical that for an entity to be an authority of the government it must exercise some governmental authority.”) (emphasis omitted); *Webster’s Third New International Dictionary* 146 (1993) (defining “authority” as “superiority derived from a status that carries with it the right to command and give final decisions”). Thus, section 106(c)’s notification requirement would generally be applicable in an ARC adjudication if that adjudication is a “trial, hearing, or other proceeding.” 50 U.S.C. § 1806(c). Although we are not aware of any judicial precedent discussing whether an employment-related administrative process such as an ARC adjudication would be a “trial, hearing, or other proceeding” for purposes of either section 106(c) or analogous, similarly worded notice statutes, we believe the ordinary meaning of the statutory language encompasses such an adjudication, and the legislative history is consistent with our understanding.

We consider first whether the ARC process is a “proceeding” within the meaning of section 106(c). *Id.* The term “proceeding” has several broad definitions, including, most

Applicability of FISA's Notification Provision to Security Clearance Adjudications

importantly for present purposes, a “procedural means for seeking redress from a tribunal or agency.” *Black’s Law Dictionary* 1324 (9th ed. 2009); *see also Webster’s Third New International Dictionary* at 1807 (defining “proceeding” as “a particular step or series of steps adopted for doing or accomplishing something”); *Random House Dictionary of the English Language* 1542 (2d ed. 1987) (defining “proceeding” as “a particular action or course or manner of action”). In order for that term to have some independent effect in section 106(c)—which we assume Congress intended, *see, e.g., Carciere v. Salazar*, 129 S. Ct. 1058, 1066 (2009) (“we are obliged to give effect, if possible, to every word Congress used”) (quoting *Reiter v. Sonotone Corp.*, 442 U.S. 330, 339 (1979))—the term “other proceeding” in section 106(c) is best read to include processes “before any court, department, officer, agency, regulatory body, or other authority of the United States” that are distinct from, and in addition to, trials and hearings. *See* 50 U.S.C. § 1806(c). The reference to proceedings before a “department, officer, agency, regulatory body, or other authority” strongly suggests that Congress did not intend to limit the application of this provision to judicial proceedings. *See id.* Accordingly, although we need not determine the outer bounds of the meaning of “proceeding,” the breadth of the dictionary definition of the term and the surrounding text in section 106(c) lead us to believe that “proceeding” would encompass the ARC’s process for adjudicating an appeal from a decision by a Department of Justice component to revoke an employee’s security clearance.

The legislative history is consistent with this broad reading of “proceeding.” When proposed legislation concerning electronic surveillance for foreign intelligence purposes was introduced in 1976, the original version of section 106(c) would have limited its scope to a “trial, hearing, or other proceeding in a Federal or State court,” S. Rep. No. 94-1035, at 64 (1976); S. Rep. No. 94-1161, at 41, 65 (1976). When a revised version of the bill was introduced in the next Congress, the language was altered to cover non-judicial proceedings expressly, *see* S. Rep. No. 95-604, at 56 (1977) (“This provision has been broadened in S. 1566 over its counterpart in S. 3197 by including non-judicial proceedings.”).⁷ To be sure, some of the language used in the relevant congressional reports echoes language used in the context of trials or court proceedings. *See, e.g.,* H.R. Rep. No. 95-1720, at 31 (1978) (Conf. Rep.) (explaining that the Senate bill “provided for notification to the court when information derived from electronic surveillance is to be used in legal proceedings”); *id.* (explaining that early notice would allow for “the disposition of any motions concerning evidence derived from electronic surveillance”); S. Rep. No. 95-701, at 62 (1978) (explaining that the notice provision, as well as the provisions governing motions for suppression, “establish the procedural mechanisms by which such information may be used in *formal* proceedings”) (emphasis added); H.R. Rep. No. 95-1283, pt. I, at 89 (1978) (same). Nevertheless, Congress’s decision to eliminate the reference to federal or state courts in the statutory provision, coupled with the legislative history’s explicit

⁷ The relevant draft statutory language discussed in Senate Report 95-604 is similar, although not identical to, the language actually passed a year later. The revised language proposed in 1977 did not explicitly include proceedings before a “regulatory body,” and would have applied not only to authorities of the United States, but also to those of a State or political subdivision. *See* S. Rep. No. 95-604, at 80. In 1978, the House Permanent Select Committee on Intelligence proposed the language that was adopted later that year and remains the current statutory text—adding the reference to “regulatory body” and focusing the section on federal authorities. *See* H.R. Rep. No. 95-1283, pt. I, at 9 (1978). Although the House Report setting out the language of section 106(c) as finally adopted explains that the notice requirements are imposed on the States through a separate section, it does not provide a reason for the change, nor does it explain the reason for the addition of the term “regulatory body.” *See id.* at 89.

Opinions of the Office of Legal Counsel in Volume 35

statement that the terms “trial, hearing, or other proceeding” were not limited to judicial proceedings, indicates that references to legal proceedings in the legislative history should not be understood as limiting section 106(c)’s reach to court proceedings.⁸

In sum, Congress’s expansion of the language of section 106(c) supports the broad reading indicated by the plain meaning of the phrase “other proceeding,”⁹ and we conclude that an ARC adjudication of a Department component’s revocation of an employee’s security clearance is an “other proceeding” within the meaning of FISA’s notification provision.¹⁰ Section 106(c) thus generally requires the Government to notify an “aggrieved person” when it intends to use information “obtained or derived from . . . electronic surveillance of that aggrieved person” against that person in such an ARC adjudication.¹¹ 50 U.S.C. § 1806(c).

⁸ Analogous provisions in the statutory scheme governing wiretaps for law enforcement purposes also strongly suggest that Congress intended the phrase “trial, hearing, or other proceeding” to be quite broad. In one provision, using language nearly identical in relevant part to that in section 106(c), Congress authorized any “aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States” to “move to suppress the contents” of interceptions. 18 U.S.C. § 2518(10)(a) (2006). According to the legislative history, “the scope of the provision [wa]s intended to be comprehensive,” although it would not include grand jury proceedings or Congressional hearings. S. Rep. No. 90-1097, at 106 (1968). The statutory scheme in the law enforcement context uses the narrower phrase—rejected in the FISA notification provision—“trial, hearing, or other proceeding in a Federal or State court” to require that certain information be provided to parties before the contents of a wiretap are used in such proceedings. 18 U.S.C. § 2518(9) (2006). The legislative history of that provision makes clear that the phrase was limited to “adversary type hearings,” and would not include a grand jury hearing. S. Rep. No. 90-1097, at 105.

⁹ Whether the term “proceeding” as used in section 106(c) refers only to an adversarial process is a question we need not decide. Cf. *In re Grand Jury Proceedings*, 856 F.2d 685, 690 & n.9 (4th Cir. 1988) (concluding that notice under section 106(c) was not required in the grand jury context because Congress explicitly included grand juries in certain provisions governing domestic wiretaps, demonstrating that Congress “knew how to include grand jury investigations as proceedings before which notice must be given to overheard persons” and because the legislative history of the domestic wiretap provisions demonstrated that “the term ‘proceeding’ was limited to include only adversary hearings”). The ARC adjudication at issue here is distinguishable from a federal grand jury proceeding because it is an adversarial process in which both sides are provided an opportunity to present their cases to a decision-maker. See 28 C.F.R. § 17.47.

¹⁰ Because we conclude that the ARC process is an “other proceeding,” we need not decide whether it is also a “hearing.” We note, however, that the term “hearing” can—and in federal law often does—refer to any “opportunity to be heard or to present one’s side of a case.” *Webster’s Third New International Dictionary* at 1044; see also *Black’s Law Dictionary* at 788 (defining a “hearing” for purposes of administrative law as “[a]ny setting in which an affected person presents arguments to a decision-maker”); 1 Richard J. Pierce, Jr., *Administrative Law Treatise* § 8.2, at 708-12 (5th ed. 2010) (collecting and discussing decisions giving deference to various agency interpretations of statutory requirements for a “hearing”). Although the term may in some instances refer specifically to a particular stage of litigation, see *Black’s Law Dictionary* at 788 (defining a “hearing” as “[a] judicial session, usu. open to the public, held for the purpose of deciding issues of fact or of law, sometimes with witnesses testifying”), or to the sort of formal, adversary process that ordinarily characterizes a trial, these are not its only meanings. Thus, an ARC adjudication may be a “hearing” as well as a “proceeding.”

¹¹ Section 106 does not specify the form of notice the Government must provide to an “aggrieved person.” See David S. Kris & J. Douglas Wilson, *National Security Investigations and Prosecutions* § 27:11 (2007) (comparing section 106(c) to other statutory search notice requirements). We have been informed that the ordinary Government practice is simply to state without elaboration that the United States intends to offer into evidence, or otherwise use or disclose, information obtained or derived from electronic surveillance conducted pursuant to FISA, and not in the first instance to provide any further information, such as the identity of the FISA target, what communications were intercepted, when the information was obtained, or what FISA information the government intends to use. See Caproni Memo at 2-3. You have not asked us to address the scope of the required notification.

*Applicability of FISA's Notification Provision to Security Clearance Adjudications***III.**

Finally, we address a constitutional issue that bears on the statutory question you have asked. The FBI notes that the President's authority to control access to national security information, and thus to make security clearance determinations for Executive Branch employees, "flows primarily" from the President's constitutional powers, *Dep't of the Navy v. Egan*, 484 U.S. 518, 527 (1988), and, further, that federal employees do not have a statutory or constitutional right to a security clearance, *see id.* at 528. In light of these premises, the FBI questions "whether Congress has the legal authority to impose restrictions on the Executive's authority and decision-making process in the security clearance context," and suggests that perhaps section 106(c) is therefore unconstitutional as applied to ARC adjudications. Caproni Memo at 1-2.

We agree with the FBI that the President's constitutional authority to classify information concerning the national defense and foreign relations of the United States and to determine whether particular individuals should be given access to such information "exists quite apart from any explicit congressional grant." *Egan*, 484 U.S. at 527; *see Whistleblower Protections for Classified Disclosures*, 22 Op. O.L.C. 92, 94-99 (1998) (statement of Randolph D. Moss, Deputy Assistant Attorney General, Office of Legal Counsel, before the House Permanent Select Committee on Intelligence). But that does not imply that Congress entirely lacks authority to legislate in a manner that touches upon disclosure of classified information. *See EPA v. Mink*, 410 U.S. 73, 83 (1973) ("Congress could certainly have provided that the Executive Branch adopt new procedures [concerning information required to be kept secret in the interest of the national defense] or it could have established its own procedures—subject only to whatever limitations the Executive privilege may be held to impose upon such congressional ordering."). For example, we believe Congress's authority to regulate foreign intelligence surveillance under FISA,¹² and to regulate the terms of federal employment,¹³ does, as a general matter, permit

We note, however, that if the aggrieved person moves the relevant authority to suppress evidence or information obtained or derived from such electronic surveillance pursuant to section 106(e), section 106(f) authorizes the Attorney General to file an affidavit under oath to the district court in the same district as the authority stating "that disclosure or an adversary hearing would harm the national security of the United States." 50 U.S.C. § 1806(f) (2006). If the Attorney General files such an affidavit, the district court is to "review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted." *Id.*; *see also id.* § 1801(g) (2006) (defining "Attorney General" for purposes of FISA to include the Attorney General (or the Acting Attorney General); the Deputy Attorney General; and, upon designation by the Attorney General, the Assistant Attorney General for National Security).

¹² *See generally* Memorandum for Hon. Edward P. Boland, Chairman, House Permanent Select Comm. on Intelligence, from John M. Harmon, Assistant Attorney General, Office of Legal Counsel (Apr. 18, 1978), in *Foreign Intelligence Electronic Surveillance: Hearings on H.R. 5794, H.R. 9745, H.R. 7308, and H.R. 5632 Before the Subcomm. on Legis. of the H. Permanent Select Comm. on Intelligence*, 95th Cong. 31 (1978) (explaining that it would be "unreasonable to conclude that Congress, in the exercise of its powers in this area," could not grant courts the authority under FISA to approve the legality of the Executive's electronic surveillance); Statement on Signing S. 1566 into Law, 2 Pub. Papers of Jimmy Carter 1853-54 (Oct. 25, 1978) (explaining that FISA "clarifies the Executive's authority" and noting no constitutional objections to the Act).

¹³ *See, e.g., United Pub. Workers v. Mitchell*, 330 U.S. 75, 101 (1947); *Ex parte Curtis*, 106 U.S. 371, 372-73 (1882). Various statutes regulate the security clearance process more generally. *See* 50 U.S.C. §§ 435-438 (2006 & Supp. III 2009); 50 U.S.C. §§ 831-835 (2006) (governing employees of the National Security Agency).

Opinions of the Office of Legal Counsel in Volume 35

Congress to impose the notification requirement in section 106(c), even when that requirement reaches proceedings concerning security clearance revocations.

The doctrine of separation of powers, however, places some limits on Congress's authority to participate in regulating the system for protecting classified information. The key question in identifying such limits is whether Congress's action is "of such a nature that [it] impede[s] the President's ability to perform his constitutional duty." *Morrison v. Olson*, 487 U.S. 654, 691 (1988). Congress may not, for example, provide Executive Branch employees with independent authority to countermand or evade the President's determinations as to when it is lawful and appropriate to disclose classified information. See *Whistleblower Protections for Classified Disclosures*, 22 Op. O.L.C. at 100. And, as noted above, Congress's authority is "subject only to whatever limitations the Executive privilege may be held to impose upon such congressional ordering." *Mink*, 410 U.S. at 83 (citing *United States v. Reynolds*, 345 U.S. 1 (1953)).

Section 106(c), by reaching broadly to require notice in proceedings such as ARC adjudications, could give rise to as-applied constitutional concerns under this separation-of-powers framework. There may, for example, be cases in which providing notice under section 106(c) would effectively disclose sensitive national security information that is constitutionally privileged. Cf. *Whistleblower Protections for Classified Disclosures*, 22 Op. O.L.C. at 94-99 (noting historical examples of presidential claims of constitutional privilege to protect national security information). Given our understanding that the information provided when notice is required by section 106(c) is quite limited, see *supra* n. 11, we expect such as-applied concerns will arise infrequently.

/s/

CAROLINE D. KRASS
Principal Deputy Assistant Attorney General

Exhibit 14

U.S.

A Secret Surveillance Program Proves Challengeable in Theory Only

Adam Liptak

SIDEBAR JULY 15, 2013

WASHINGTON — On Oct. 29, about seven months before the recent revelations about secret government surveillance programs, Solicitor General Donald B. Verrilli Jr. made a commitment to the Supreme Court.

It was on the day Hurricane Sandy shut down the rest of Washington. The justices had made it to court through lashing rain, and they seemed to be paying particular attention when Mr. Verrilli, the Obama administration's top appellate lawyer, argued that a challenge to a 2008 surveillance law should be dismissed.

He said, a little comically in retrospect, that the human rights groups, lawyers and reporters who sought to challenge the law had no particular reason to think that their communications were being collected. The plaintiffs could not show they had been harmed by the surveillance program, he said, so they lacked standing to sue. Their fears, he said, were the product of "a cascade of speculation."

That was merely aggressive and effective advocacy.

Mr. Verrilli's responses to the first several questions at the argument have turned out to be more problematic. He was asked whether a ruling in the government's favor would mean that no court could ever assess the constitutionality of the program.

“Is there anybody who has standing?” Justice Sonia Sotomayor asked.

Yes, said Mr. Verrilli, giving what he called a “clear example.” If the government wants to use information gathered under the surveillance program in a criminal prosecution, he said, the source of the information would have to be disclosed. The subjects of such surveillance, he continued, would have standing to challenge the program.

Mr. Verrilli said this pretty plainly at the argument and even more carefully in his briefs in the case.

In one brief, for example, he sought to refute the argument that a ruling in the government’s favor would immunize the surveillance program from constitutional challenges.

“That contention is misplaced,” he wrote. “Others may be able to establish standing even if respondents cannot. As respondents recognize, the government must provide advance notice of its intent to use information obtained or derived from” the surveillance authorized by the 2008 law “against a person in judicial or administrative proceedings and that person may challenge the underlying surveillance.” (Note the phrase “derived from.”)

In February, in a 5-to-4 decision that split along ideological lines, the Supreme Court accepted Mr. Verrilli’s assurances and ruled in his favor. Justice Samuel A. Alito Jr., writing for the majority in the case, *Clapper v. Amnesty International*, all but recited Mr. Verrilli’s representation.

“If the government intends to use or disclose information obtained or derived from” surveillance authorized by the 2008 law “in judicial or administrative proceedings, it must provide advance notice of its intent, and the affected person may challenge the lawfulness of the acquisition.” (Again, note the phrase “derived from.”)

What has happened since then in actual criminal prosecutions? The opposite of what Mr. Verrilli told the Supreme Court. Federal prosecutors, apparently unaware of his representations, have refused to make the promised disclosures.

In a prosecution in Federal District Court in Fort Lauderdale, Fla., against two brothers accused of plotting to bomb targets in New York, the government has said it plans to use information gathered under the Foreign Intelligence Surveillance Act of 1978, or FISA, which authorized individual warrants. But prosecutors have refused to say whether the government obtained those individual warrants based on information derived from the 2008 law, which allows programmatic surveillance.

Prosecutors in Chicago have taken the same approach in a prosecution of teenager accused of plotting to blow up a bar.

In the Fort Lauderdale case, Magistrate Judge John J. O'Sullivan ordered the government to disclose whether it had gathered information for the case under the 2008 law. He relied on Justice Alito's statement in the Clapper decision. The government has moved for reconsideration.

By insisting that they need not disclose whether there had been surveillance under the 2008 law, the two sets of prosecutors have so far accomplished precisely what Mr. Verrilli said would not happen. They have immunized the surveillance program from challenges under the Fourth Amendment, which bans unreasonable searches and seizure.

Yet there is excellent reason to think that surveillance under the 2008 law, the FISA Amendments Act, was involved in both cases. In December, in explaining why the law should be reauthorized, Senator Dianne Feinstein, Democrat of California, said the Fort Lauderdale and Chicago cases were among the "specific cases where FISA Amendments Act authorities were used."

"These cases show the program has worked," she said.

Michelle Alvarez, a spokeswoman for the United States attorney's office in Miami, would not say whether prosecutors there had consulted with the Justice Department in Washington before taking a position that seems at odds with Mr. Verrilli's assurances to the Supreme Court. Neither would Randall Samborn, a spokesman for the United States attorney's office in Chicago.

A Justice Department spokesman in Washington said things might yet change in the two cases. “The legal issues raised in the filings are under active consideration within the department,” he said.

Jameel Jaffer, the American Civil Liberties Union lawyer who represented the plaintiffs in the Clapper case in the Supreme Court, said the recent maneuvers were unseemly and disturbing. “The effect of the government’s shell game,” he said, “is that the statute has been shielded from judicial review, and controversial and far-reaching surveillance authorities have been placed beyond the reach of the Constitution.”

Whatever the government’s precise legal obligations, it remains free to say what everyone seems to know: that the 2008 program has been used to gather evidence for criminal prosecutions. Such a concession would seem to be a small thing. All it would do is allow the courts to make a judgment about whether the program is constitutional.

A version of this article appears in print on July 16, 2013, on Page A11 of the New York edition with the headline: A Secret Surveillance Program Proves Challengeable in Theory Only.

Exhibit 15

turn, must review the targeting and minimization procedures to ensure that they satisfy the statutory criteria and are consistent with the Fourth Amendment. 50 U.S.C. 1881a(i)(2)(B), (C) and (3)(A).

Section 1881a further requires that the Attorney General and Director of National Intelligence periodically assess the government's compliance with both the targeting and minimization procedures and with relevant compliance guidelines, and that they submit those assessments both to the FISC and to congressional oversight committees. 50 U.S.C. 1881a(l). The Attorney General must also keep the relevant oversight committees "fully inform[ed]" concerning the implementation of Section 1881a. 50 U.S.C. 1881f(a) and (b)(1).

If the government intends to use or disclose any information obtained or derived from its acquisition of a person's communications under Section 1881a in judicial or administrative proceedings against that person, it must provide advance notice of its intent to the tribunal and the person, whether or not the person was targeted for surveillance under Section 1881a. 50 U.S.C. 1881e(a); see 50 U.S.C. 1801(k), 1806(c). That person may then challenge the use of that information in district court by challenging the lawfulness of the Section 1881a acquisition. 50 U.S.C. 1806(e) and (f), 1881e(a). Separately, any electronic service provider the government directs to assist in Section 1881a surveillance may challenge the lawfulness of that directive in the FISC. 50 U.S.C. 1881a(h)(4) and (6); cf. Pet. App. 144a-145a.⁶

⁶ Cf. also, *e.g.*, *In re Directives*, 551 F.3d 1004 (FISC Rev. 2008) (adjudicating Fourth Amendment challenge brought by electronic service provider to directive issued under Section 1881a's predecessor provisions in the Protect America Act of 2007, Pub. L. No. 110-55, secs. 2-3, §§ 105A-105C, 121 Stat. 552-555 (50 U.S.C. 1805a-1805c (Supp. I 2007))

Exhibit 16

Official

1 IN THE SUPREME COURT OF THE UNITED STATES

2 - - - - - x

3 JAMES R. CLAPPER, JR., DIRECTOR :

4 OF NATIONAL INTELLIGENCE, ET AL., :

5 Petitioners : No. 11-1025

6 v. :

7 AMNESTY INTERNATIONAL USA, ET AL. :

8 - - - - - x

9 Washington, D.C.

10 Monday, October 29, 2012

11

12 The above-entitled matter came on for oral
13 argument before the Supreme Court of the United States
14 at 10:03 a.m.

15 APPEARANCES:

16 DONALD B. VERRILLI, JR., ESQ., Solicitor General,
17 Department of Justice, Washington, D.C.; on behalf of
18 Petitioners.

19 JAMEEL JAFFER, ESQ., New York, New York; on behalf of
20 Respondents.

21

22

23

24

25

Official

	C O N T E N T S	
1		
2	ORAL ARGUMENT OF	PAGE
3	DONALD B. VERRILLI, JR., ESQ.	
4	On behalf of the Petitioners	3
5	ORAL ARGUMENT OF	
6	JAMEEL JAFFER, ESQ.	
7	On behalf of the Respondents	27
8	REBUTTAL ARGUMENT OF	
9	DONALD B. VERRILLI, JR., ESQ.	
10	On behalf of the Petitioners	56
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		

Official

1 P R O C E E D I N G S

2 (10:03 a.m.)

3 CHIEF JUSTICE ROBERTS: We'll hear argument
4 first this morning in Case 11-1025, Clapper v. Amnesty
5 International.

6 General Verrilli.

7 ORAL ARGUMENT OF DONALD B. VERRILLI, JR.,

8 ON BEHALF OF THE PETITIONERS

9 GENERAL VERRILLI: Mr. Chief Justice, and
10 may it please the Court:

11 The question in this case is whether
12 Respondents have standing to bring a facial challenge to
13 the 2008 amendments to the Foreign Intelligence
14 Surveillance Act. Those amendments provide authority to
15 the executive to conduct surveillance targeted at
16 foreign persons located abroad for foreign intelligence
17 purposes.

18 Along with that grant of authority, Congress
19 imposed statutory protections designed --

20 JUSTICE SOTOMAYOR: General, is there
21 anybody who has standing?

22 As I read your brief, standing would only
23 arise at the moment the government decided to use the
24 information against someone in a pending case. To me,
25 that --

Official

1 GENERAL VERRILLI: Several points,
2 Your Honor --

3 JUSTICE SOTOMAYOR: -- would seem to say
4 that the Act -- if there were a violation; I'm not
5 suggesting there is -- but that if there was a
6 constitutional violation in the interception, that no
7 one could ever stop it until they were charged with a
8 crime, essentially.

9 GENERAL VERRILLI: Your Honor, under the
10 statute, there are two clear examples of situations in
11 which the individuals would have standing.

12 The first is if an aggrieved person, someone
13 who is a party to a communication, gets notice that the
14 government intends to introduce information in a
15 proceeding against them. They have standing. That
16 standing could include a facial challenge like the one
17 here.

18 JUSTICE GINSBURG: General Verrilli, can you
19 be specific on who that person would be? Because, as I
20 understand it, it's unlikely that, for example, the
21 lawyers in this case would be charged with any criminal
22 offense. It's more probable that their clients would
23 be; but, according to the government, their clients have
24 no Fourth Amendment rights because they are people who
25 are noncitizens who acted abroad.

Official

1 So it's hard for me to envision. I see the
2 theoretical possibility, but I don't see a real person
3 who would be subject to a criminal charge who could
4 raise an objection.

5 GENERAL VERRILLI: Well, if the
6 information were -- if anyone gets notice, including the
7 client, then the lawyer would know, and the lawyer would
8 be in a position at that point to act.

9 JUSTICE GINSBURG: So the client is somebody
10 who is abroad and who acted abroad, and is not a U.S.
11 citizen.

12 GENERAL VERRILLI: That's certainly true.
13 But, in addition, Your Honor, the statute provides that
14 -- that electronic communication service providers can
15 challenge authorizations under the Act, so you -- there
16 certainly would be standing in that instance.

17 There was such a case.

18 JUSTICE GINSBURG: How likely is it that a
19 service provider would object?

20 GENERAL VERRILLI: Well, the service
21 provider did object to the immediate statutory
22 predecessor to the 2008 amendments. And the -- and the
23 FISA court litigated that constitutional challenge. So
24 there's a concrete context there in which it arises.
25 But even -- but beyond that --

Official

1 JUSTICE GINSBURG: And the litigation was
2 unsuccessful.

3 GENERAL VERRILLI: Well, that's right. The
4 Court found there was no Fourth Amendment violation
5 there.

6 But I think the point here, Your Honor,
7 is -- the key point is this, that the -- in a normal
8 case, a plaintiff would challenge the application of the
9 authority to that plaintiff. In a situation like this
10 one, we acknowledge that it may be difficult for a
11 plaintiff to do so because an -- a challenge to the
12 application gets into classified information pretty
13 quickly.

14 I think what the Respondents have tried to
15 do here is to find a theory of the case that avoids that
16 difficulty.

17 JUSTICE GINSBURG: Well, using what you just
18 mentioned, suppose -- just let's suppose that the Court
19 should hold there is standing. Couldn't the government
20 then say as far as the merits of the complaint, this
21 information is classified, these are state secrets, we
22 can't -- we can't go forward with the litigation?

23 GENERAL VERRILLI: That is a possibility.
24 Of course, there's a procedure that the executive branch
25 would have to go through, but that's a possibility.

Exhibit 17

POLITICS

Door May Open for Challenge to Secret Wiretaps

By CHARLIE SAVAGE OCT. 16, 2013

WASHINGTON — Five years after Congress authorized a sweeping warrantless surveillance program, the Justice Department is setting up a potential Supreme Court test of whether it is constitutional by notifying a criminal defendant — for the first time — that evidence against him derived from the eavesdropping, according to officials.

Prosecutors plan to inform the defendant about the monitoring in the next two weeks, a law enforcement official said. The move comes after an internal Justice Department debate in which Solicitor General Donald B. Verrilli Jr. argued that there was no legal basis for a previous practice of not disclosing links to such surveillance, several Obama administration officials familiar with the deliberations said.

Meanwhile, the department's National Security Division is combing active and closed case files to identify other defendants who faced evidence resulting from the 2008 wiretapping law. It permits eavesdropping without warrants on Americans' cross-border phone calls and e-mails so long as the surveillance is "targeted" at foreigners abroad.

It is not yet clear how many other such cases there are, nor whether prosecutors will notify convicts whose cases are already over. Such a decision could set off attempts to reopen those cases.

“It’s of real legal importance that components of the Justice Department disagreed about when they had a duty to tell a defendant that the surveillance program was used,” said Daniel Richman, a Columbia University law professor. “It’s a big deal because one view covers so many more cases than the other, and this is an issue that should have come up repeatedly over the years.”

The officials spoke on the condition of anonymity because they were not authorized to disclose internal discussions. **The Wall Street Journal** previously reported on a recent court filing in which the department, reversing an earlier stance, said it was obliged to disclose to defendants if evidence used in court was linked to warrantless surveillance, but it remained unclear if there were any such cases.

The debate was part of the fallout about National Security Agency surveillance set off by leaks by Edward J. Snowden, the former N.S.A. contractor. They have drawn attention to the 2008 law, the FISA Amendments Act, which legalized a form of the Bush administration’s once-secret warrantless surveillance program.

In February, the Supreme Court dismissed a case challenging its constitutionality because the plaintiffs, led by Amnesty International, could not prove they had been wiretapped. Mr. Verrilli had told the justices that someone else would have legal standing to trigger review of the program because prosecutors would notify people facing evidence derived from surveillance under the 2008 law.

But it turned out that Mr. Verrilli’s assurances clashed with the practices of national security prosecutors, who had not been alerting such defendants that evidence in their cases had stemmed from wiretapping their conversations without a warrant.

Jameel Jaffer, an American Civil Liberties Union lawyer who argued in the Supreme Court on behalf of the plaintiffs challenging the 2008 law, said that someone in the Justice Department should have flagged the issue earlier and that the department must do more than change its practice going forward.

“The government has an obligation to tell the Supreme Court, in some formal way, that a claim it made repeatedly, and that the court relied on in its decision, was simply not true,” he said. “And it has an obligation to notify the criminal defendants whose communications were monitored under the statute that their communications were monitored.”

A Justice Department spokesman declined to comment. The department’s practices came under scrutiny after a December 2012 speech by Senator Dianne Feinstein, the chairwoman of the Intelligence Committee. During debate over extending the 2008 law, she warned that terrorism remained a threat. Listing several terrorism-related arrests, she added, “so this has worked.”

Lawyers in two of the cases Ms. Feinstein mentioned — one in Fort Lauderdale and one in Chicago — asked prosecutors this spring to confirm that surveillance under the 2008 law had played a role in the investigations of their clients so they could challenge it.

But prosecutors said they did not have to make such a disclosure. On June 7, The New York Times published an article citing Ms. Feinstein’s speech and the stance the prosecutors had taken.

As a result, Mr. Verrilli sought an explanation from national security lawyers about why they had not flagged the issue when vetting his Supreme Court briefs and helping him practice for the arguments, according to officials.

The national security lawyers explained that it was a misunderstanding, the officials said. Because the rules on wiretapping warrants in foreign intelligence cases are different from the rules in ordinary criminal investigations, they said, the division has long used a narrow understanding of what “derived from” means in terms of when it must disclose specifics to defendants.

In national security cases involving orders issued under the Foreign Intelligence Surveillance Act of 1978, or FISA, prosecutors alert defendants only that some evidence derives from a FISA wiretap, but not details like whether there had just been one order or a chain of several. Only judges see those details.

After the 2008 law, that generic approach meant that prosecutors did not disclose when some traditional FISA wiretap orders had been obtained using information gathered through the warrantless wiretapping program. Division officials believed it would have to disclose the use of that program only if it introduced a recorded phone call or intercepted e-mail gathered directly from the program — and for five years, they avoided doing so.

For Mr. Verrilli, that raised a more fundamental question: was there any persuasive legal basis for failing to clearly notify defendants that they faced evidence linked to the 2008 warrantless surveillance law, thereby preventing them from knowing that they had an opportunity to argue that it derived from an unconstitutional search?

The debate stretched through June and July, officials said, including multiple meetings and dueling memorandums by lawyers in the solicitor general office and in the national security division, which has been led since March by acting Assistant Attorney General John Carlin. The deliberations were overseen by James Cole, the deputy attorney general.

National security lawyers and a policy advisory committee of senior United States attorneys focused on operational worries: Disclosure risked alerting foreign targets that their communications were being monitored, so intelligence agencies might become reluctant to share information with law enforcement officials that could become a problem in a later trial.

But Mr. Verrilli argued that withholding disclosure from defendants could not be justified legally, officials said. Lawyers with several agencies — including the Federal Bureau of Investigation, the N.S.A. and the office of the director of national intelligence — concurred, officials said, and the division changed the practice going forward.

National Security Division lawyers began looking at other cases, eventually identifying the one that will be publicly identified soon and are still looking through closed cases and deciding what to do about them.

But in a twist, in the Chicago and Fort Lauderdale cases that Ms. Feinstein had mentioned, prosecutors made new court filings saying they did not intend to use any evidence derived from surveillance of the defendants under the 2008 law.

When defense lawyers asked about Ms. Feinstein's remarks, a Senate lawyer responded in a letter that she "did not state, and did not mean to state" that those cases were linked to the warrantless surveillance program. Rather, the lawyer wrote, her point was that terrorism remained a problem.

In a recent court filing, the lawyers wrote that it is "hard to believe" Ms. Feinstein would cite "random" cases when pressing to reauthorize the 2008 law, suggesting either that the government is still concealing something or that she had employed the "politics of fear" to influence the debate. A spokesman for Ms. Feinstein said she preferred to let the letter speak for itself.

A version of this article appears in print on October 17, 2013, on Page A3 of the New York edition with the headline: Door May Open for Challenge to Secret Wiretaps.

Exhibit 18

U.S.

Federal Prosecutors, in a Policy Shift, Cite Warrantless Wiretaps as Evidence

By CHARLIE SAVAGE OCT. 26, 2013

WASHINGTON — The Justice Department for the first time has notified a criminal defendant that evidence being used against him came from a warrantless wiretap, a move that is expected to set up a Supreme Court test of whether such eavesdropping is constitutional.

Prosecutors filed such a notice late Friday in the case of Jamshid Muhtorov, who was charged in Colorado in January 2012 with providing material support to the Islamic Jihad Union, a designated terrorist organization based in Uzbekistan.

Mr. Muhtorov is accused of planning to travel abroad to join the militants and has pleaded not guilty. A criminal complaint against him showed that much of the government's case was based on intercepted e-mails and phone calls.

The government's notice allows Mr. Muhtorov's lawyer to ask a court to suppress the evidence by arguing that it derived from unconstitutional surveillance, setting in motion judicial review of the eavesdropping.

The New York Times reported on Oct. 17 that the decision by prosecutors to notify a defendant about the wiretapping followed a legal policy debate inside the Justice Department.

The debate began in June when Solicitor General Donald B. Verrilli Jr. discovered that the department's National Security Division did not notify criminal defendants when eavesdropping without a warrant was an early link in an investigative chain that led to evidence used in court. As a result, none of the defendants knew that they had the right to challenge the warrantless wiretapping law.

The practice contradicted what Mr. Verrilli had told the Supreme Court last year in a case challenging the law, the FISA Amendments Act of 2008. Legalizing a form of the Bush administration's program of warrantless surveillance, the law authorized the government to wiretap Americans' e-mails and phone calls without an individual court order and on domestic soil so long as the surveillance is "targeted" at a foreigner abroad.

A group of plaintiffs led by Amnesty International had challenged the law as unconstitutional. But Mr. Verrilli last year urged the Supreme Court to dismiss the case because those plaintiffs could not prove that they had been wiretapped. In making that argument, he said a defendant who faced evidence derived from the law would have proper legal standing and would be notified, so dismissing the lawsuit by Amnesty International would not close the door to judicial review of the 2008 law. The court accepted that logic, voting 5-to-4 to dismiss the case.

In a statement, Patrick Toomey, staff attorney with the American Civil Liberties Union, which had represented Amnesty International and the other plaintiffs, hailed the move but criticized the Justice Department's prior practice.

"We welcome the government's belated recognition that it must give notice to criminal defendants who it has monitored under the most sweeping surveillance law ever passed by Congress," Mr. Toomey said. "By withholding notice, the government has avoided judicial review of its dragnet warrantless wiretapping program for five years."

The Justice Department change traces back to June, when The Times reported that prosecutors in Fort Lauderdale and Chicago had told plaintiffs they did not need to say whether evidence in their cases derived from warrantless wiretapping, in conflict with what the Justice Department had told the Supreme Court.

After reading the article, Mr. Verrilli sought an explanation from the National Security Division, whose lawyers had vetted his briefs and helped him practice for his arguments, according to officials with knowledge of the internal deliberations. It was only then that he learned of the division's practice of narrowly interpreting its need to notify defendants of evidence "derived from" warrantless wiretapping.

There ensued a wider debate throughout June and July, the officials said. National security prosecutors raised operational concerns: disclosing more to defendants could tip off a foreign target that his communications were being monitored, so intelligence officials might become reluctant to share crucial information that might create problems in a later trial.

Mr. Verrilli was said to have argued that there was no legal basis to conceal from defendants that the evidence derived from legally untested surveillance, preventing them from knowing they had an opportunity to challenge it. Ultimately, his view prevailed and the National Security Division changed its practice going forward, leading to the new filing on Friday in Mr. Muhtorov's case.

Still, it remains unclear how many other cases — including closed matters in which convicts are already serving prison sentences — involved evidence derived from warrantless wiretapping in which the National Security Division did not provide full notice to defendants, nor whether the department will belatedly notify them. Such a notice could lead to efforts to reopen those cases.

Correction: October 27, 2013

An earlier version of this article incorrectly stated that a criminal complaint showed that much of the government's case against Jamshid Muhtorov was based on e-mails and phone calls intercepted under a 2008 surveillance law. The complaint does not say that the particular communications it cites were obtained directly from such surveillance.

A version of this article appears in print on October 27, 2013, on Page A21 of the New York edition with the headline: U.S. Prosecutors Cite Warrantless Wiretaps.

Exhibit 19

EMN:SDD
F.#2011R00783

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----- X

AGRON HASBAJRAMI

- against -

13 CV 6852 (JG)

UNITED STATES OF AMERICA,

Respondent.

----- X

MEMORANDUM IN OPPOSITION TO MOTION TO COMPEL DISCOVERY

LORETTA E. LYNCH
United States Attorney
Eastern District of New York
271 Cadman Plaza East
Brooklyn, New York 11201

Seth D. DuCharme
Assistant U.S. Attorney
(Of Counsel)

JOHN P. CARLIN
Assistant Attorney General
For National Security

Alexis Collins
Trial Attorney
Counterterrorism Section
U.S. Department of Justice

TABLE OF CONTENTS

	<u>Page</u>
TABLE OF AUTHORITIES	iii
PRELIMINARY STATEMENT	1
I. BACKGROUND	4
II. APPLICABLE LAW	8
A. The Foreign Intelligence Surveillance Act	9
B. Collateral Proceedings under 28 U.S.C. § 2255	10
1. A Section 2255 Petitioner Must Show That The Discovery He Seeks Would Establish a Legal Claim That Would Entitle Him To Relief	10
2. Effect of Guilty Plea	12
C. Discovery Standards	13
ARGUMENT	14
I. HASBAJRAMI HAS NO RIGHT TO DISCOVERY ON COLLATERAL ATTACK....	14
A. Hasbajrami has not raised a substantive claim.	15
B. Hasbajrami would not be entitled to relief based on the discovery he seeks	16
1. Hasbajrami’s Guilty Plea Forecloses His Constitutional and Statutory Challenges to the Legality of the Section 702 Collection.....	17
2. The Discovery Hasbajrami Seeks Relating to the Supplemental Notification Does Not Implicate the Validity of his Plea	20
II. HASBAJRAMI CANNOT JUSTIFY DISCLOSURE OF THE REQUESTED MATERIALS ON ANY OTHER BASIS.....	24
A. Hasbajrami fails to establish government misconduct.....	24
B. The timing of the Supplemental Notification is not indicative of bad faith.	25
III. THE MATERIALS HASBAJRAMI SEEKS ARE PROTECTED BY THE ATTORNEY CLIENT AND DELIBERATIVE PROCESS PRIVILEGES	31

IV. THERE IS NO BASIS TO ORDER DISCOVERY OF CLASSIFIED MATERIALS
RELATING TO THE
AUTHORIZATION OR EXECUTION OF SECTION 702 COLLECTION BECAUSE
THE LAWFULNESS
OF THE COLLECTION IS NOT BEFORE THE COURT 33

V. DEFENSE COUNSEL’S SECURITY CLEARANCES ARE NOT A DETERMINATIVE
OR LAWFUL
BASIS UPON WHICH TO PROVIDE THE REQUESTED DISCOVERY 36

VI. HASBAJRAMI’S SWEEPING ALLEGATIONS RELATING TO GOVERNMENT
SURVEILLANCE
PROGRAMS ARE NOT GROUNDED IN THE RECORD..... 38

CONCLUSION..... 39

TABLE OF AUTHORITIES

<u>Cases</u>	<u>Page</u>
<u>Amparo v. Henderson</u> , No. 86 Civ. 4310, 1989 WL 126831.....	12
<u>Beatty v. Greiner</u> , 50 Fed. Appx. 494 (2d Cir. 2002).....	12
<u>Bousley v. United States</u> , 523 U.S. 614 (1998).....	22
<u>Bracy v. Gramley</u> , 520 U.S. 899 (1997).....	10, 14, 22
<u>Brady v. Maryland</u> , 373 U.S. 83 (1963).....	13
<u>Clapper v. Amnesty Int’l USA</u> , 133 S. Ct. 1138 (2013).....	28
<u>Clark v. Johnson</u> , 202 F.3d 760 (5th Cir. 2000)	11
<u>Czernicki v. United States</u> , 270 F. Supp. 2d 391 (S.D.N.Y. 2003)	19
<u>Davis v. United States</u> , 131 S. Ct. 2419 (2011).....	35
<u>Deputy v. Taylor</u> , 19 F.3d 1485 (3rd Cir.1994)	11
<u>Ferrara v. United States</u> , 384 F. Supp. 2d 384 (D. Mass. 2005).....	12
<u>Giglio v. United States</u> , 405 U.S. 150 (1972).....	13
<u>Graziano v. United States</u> , 83 F.3d 587 (2d Cir. 1996)	17
<u>Haring v. Prosise</u> , 462 U.S. 306 (1983).....	18
<u>Harris v. Johnson</u> , 81 F.3d 535 (5th Cir.1996)	11

Harris v. Nelson,
394 U.S. 286 (1969)..... 10

Hill v. Johnson,
210 F.3d 481 (5th Cir. 2000) 11

Hubanks v. Frank,
392 F.3d 926 (7th Cir. 2004) 11

In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act,
551 F.3d 1004 (FISC Ct. Rev. 2008)..... 30

In re Sealed Case,
121 F.3d 729 (D.C. Cir. 1997)..... 31

Lugo v. Artus,
No. 05 Civ. 1998 (SAS), 2008 WL 312298 (S.D.N.Y. Jan. 31, 2008)..... 12

Murphy v. Johnson,
205 F.3d 809 (5th Cir. 2000) 11

Newton v. Kemna,
354 F.3d 776 (8th Cir. 2004) 11, 17

Puglisi v. United States,
586 F.3d 209 (2d Cir. 2009) 15

Rich v. Calderon,
187 F.3d 1064 (9th Cir. 1999) 11

Ricketts v. Adamson,
483 U.S. 1 (1987)..... 20

Rosa v. United States,
170 F. Supp. 2d 388 (S.D.N.Y. 2001) 19

Smith v. United States,
876 F.2d 655 (8th Cir. 1989) 18

Stanford v. Parker,
266 F.3d 442 (6th Cir. 2001) 11

Stone v. Powell,
428 U.S. 465 (1976)..... 17

Strickler v. Greene,
527 U.S. 263 (1999)..... 30

Tate v. Wood,
963 F.2d 20 (2d Cir. 1992) 30, 35

Teague v. Lane,
489 U.S. 288 (1989)..... 17

Tobon v. United States,
132 F. Supp. 2d 164 (S.D.N.Y. 2001) 19

Tollett v. Henderson,
411 U.S. 258 (1973)..... 12, 17

United States v. Abu Jihaad,
630 F.3d 102 (2d Cir. 2010) 36

United States v. Abu-Jihaad,
2007 WL 2972623 (D. Conn. Oct. 11, 2007) 37

United States v. Amawi,
2009 WL 961143 (N.D. Ohio, Apr. 7, 2009)..... 37

United States v. Arango,
966 F.2d 64 (2d Cir. 1992) 18

United States v. Arenas-Ortiz,
339 F.3d 1066 (9th Cir. 2003) 13, 29

United States v. Armstrong,
517 U.S. 456 (1996)..... 13

United States v. Bin Laden,
126 F. Supp. 2d 264 (S.D.N.Y. 2000) 37

United States v. Bradley,
400 F.3d 459 (6th Cir. 2005) 16

United States v. Broce,
488 U.S. 563 (1989)..... 17, 18, 20, 21

United States v. Daoud,
755 F.3d 479 (7th Cir. 2014) 36

United States v. Duggan,
743 F.2d 59 (2d Cir. 1984) 14, 34

United States v. El-Mezain,
664 F.3d 467 (5th Cir. 2011) 14, 34, 37

United States v. Fernandez,
231 F.3d 1240 (9th Cir. 2000) 31

United States v. Fisher,
711 F.3d 460 (4th Cir. 2013) 13, 22

United States v. Gale,
314 F.3d 1 (D.C. Cir. 2003)..... 23, 24

United States v. Ghailani,
751 F. Supp. 2d 498 (S.D.N.Y. 2010) 31, 32

United States v. Gregg,
463 F.3d 160 (2d Cir. 2006) 12

United States v. Lee,
523 F.3d 104 (2d Cir. 2008) 19

United States v. Leyland,
277 F.3d 628 (2d Cir. 2002) 20

United States v. Libby,
429 F. Supp. 2d 18 (D.D.C. 2006)..... 37

United States v. Mahaffy,
693 F.3d 113 (2d Cir. 2012) 30

United States v. McLean,
419 Fed. Appx. 473 (5th Cir. 2011)..... 21

United States v. Mohamud,
, Cr. No. 3:10-00475 (KI) 2014 WL 2866749 (D. Or. June 24, 2014)..... passim

United States v. Nicholson,
721 F.3d 1236 (10th Cir. 2013) 35

United States v. Ott,
827 F.2d 473 (9th Cir. 1987) 37

United States v. Pappas,
94 F.3d 795 (2d Cir 1996) 36

United States v. Reynolds,
345 U.S. 1 (1953)..... 32

United States v. Ruiz,
536 U.S. 622 (2002)..... 12, 19, 21

United States v. Selby,
476 F.2d 965 (2d Cir. 1973) 18

United States v. Sykes,
697 F.2d 87 (2d Cir. 1983) 18

United States v. Wilson,
901 F.2d 378 (4th Cir. 1990) 12

United States v. Yousef,
327 F.3d 56 (2d Cir. 2003) 37

Statutes

18 U.S.C. § 2332a(a)(2)(A) 25
18 U.S.C. § 2339A 15
18 U.S.C. § 2339A(a) 1, 5, 6
18 U.S.C. § 3500 13
18 U.S.C. §§ 2510-2522 27
18 U.S.C. App. 3 35
28 U.S.C. § 2255 passim
50 U.S.C. § 1801(k) 9
50 U.S.C. § 1825(d) 9
50 U.S.C. § 1881a 7, 9
50 U.S.C. § 1881a(a) 9
50 U.S.C. § 1881a(b) 9
50 U.S.C. § 1881e(a) 10, 34
50 U.S.C. §§ 1801-1812 5
50 U.S.C. §§1806(c) 7, 8, 9
50 U.S.C. §1806(e) 10, 26, 35
50 U.S.C. 1806(f) 10, 13, 23, 34

PRELIMINARY STATEMENT

On April 12, 2012, petitioner/defendant Agron Hasbajrami (“Hasbajrami”) pleaded guilty to one count of attempting to provide material support to terrorists, in violation of 18 U.S.C. § 2339A(a). On January 8, 2013, the Court sentenced Hasbajrami to a 15-year term of incarceration, which he is currently serving. Thereafter, Hasbajrami filed a pro se motion seeking to vacate his conviction and sentence, principally on the ground that Section 2339A is unconstitutionally vague. The government responded and, on February 24, 2014, provided supplemental notification (the “Supplemental Notification”) based on a post-plea determination by the Department of Justice (the “Department”) and the prosecutors that certain evidence or information obtained or derived from Title I and Title III collection under the Foreign Intelligence Surveillance Act (“FISA”) in Hasbajrami’s criminal case was itself also derived from other collection pursuant to Section 702 of Title VII of FISA, codified through the FISA Amendments Act of 2008 (“FAA”), as to which Hasbajrami was aggrieved. In that notification, the government stated that it did not oppose modifying the existing briefing schedule to permit Hasbajrami to amend his Section 2255 petition.

Rather than filing an amended petition, on June 30, 2014, Hasbajrami filed a motion for discovery, seeking, inter alia, materials which he expressly agreed to forego in his plea agreement and to which he is not otherwise entitled. In sum, he primarily seeks three broad categories of materials: (1) information and records regarding a purported Department policy of non-disclosure of the use of Section 702 information and the circumstances underlying the provision of the Supplemental Notification in this case (Def’s Mot. at 9-10); (2) classified factual information relating to the Title I/III and Section 702 collection relevant to his case, including all FISA applications, orders and related materials and their content and the government’s opinion on

the legality of the Section 702 collection (id. at 8-10); and, based on newspaper articles regarding surveillance activities that have been the subject of recent public debate due to the unauthorized disclosure of classified information, (3) discovery of additional materials relating to the use of such investigative tools that he baselessly speculates may have been used against him but that otherwise have nothing to do with the Supplemental Notification (id. at 36-42).¹

Hasbajrami argues that discovery of the Department's internal deliberative records is required in order to discern an appropriate remedy for the late Supplemental Notification. (Id. at 21-27.) With respect to his request for information regarding the FISA collection, he claims that access is required in order to: (1) determine whether Hasbajrami's plea was voluntary and whether it would benefit Hasbajrami to seek to withdraw his guilty plea (id. at 6, 27); and (2) support a potential argument that Hasbajrami may make challenging the legality of the underlying Section 702 collection (id. at 30-36). He further argues that the Court should order the government to produce any classified materials to cleared defense counsel due to the "complexity" of the case and should grant "the broadest discovery" because of "important societal purposes of transparency and deterrence." (Id. at 42-66.) Although he has not filed a substantive claim with respect to his guilty plea, Hasbajrami nonetheless argues that waivers contained in his plea agreement are unenforceable due to "institutional complicity" and Constitutional principles. (Id. at 69.)

To be clear, Hasbajrami has not moved to withdraw his guilty plea, but rather wishes to engage in a fishing expedition driven by vague and unsupportable allegations of government misconduct. To obtain discovery in a Section 2255 proceeding, a petitioner must make a prima facie showing that, if discovery were allowed, he could satisfy each element of his

¹ The defendant asserts that his discovery request should extend beyond the U.S. Attorney's Office to include other U.S. government entities.

claim for relief and defeat any procedural bars that would prevent the court from reaching the merits of his claim. For the reasons set forth below, Hasbajrami cannot make that showing.

First, Hasbajrami has not yet raised any substantive claim of error related to the discovery he seeks. The principal claim that he has yet raised – a constitutional challenge to Section 2339A – has nothing to do with any of the discovery requests in the instant motion. Hasbajrami’s argument that he should get discovery up front to help him decide whether to raise additional claims is the kind of speculative “fishing expedition” request that courts have routinely rejected in collateral proceedings.

Second, even if Hasbajrami could properly obtain discovery to support claims he has not raised, his motion would still be meritless. A petitioner’s unconditional guilty plea forecloses any collateral claims based on alleged constitutional or statutory violations that occurred before the guilty plea. Accordingly, Hasbajrami may not obtain discovery of materials related to the conduct of the Section 702 collection in this case, because his guilty plea forecloses any potential claims asserting constitutional or statutory violations arising from that collection. The only potential claim identified in Hasbajrami’s motion that is not foreclosed is a challenge to the voluntariness of his plea. But even if he had filed a petition seeking to set aside his guilty plea, Hasbajrami would still not be entitled to receive the discovery he seeks, because neither internal deliberative documents regarding the provision of Section 702 notice in this or any other case nor information relating to the legality of the underlying FISA collection would assist in establishing that claim.

To the extent Hasbajrami believes he has suffered prejudice from the delay in issuing the Supplemental Notification, his legal recourse is to move to vacate his guilty plea. While the government does not believe such a motion would be meritorious, should the Court

grant such a motion, Hasbajrami would be in the same place in his case as he would have been in had the Supplemental Notification been provided before his plea. That is, he would then have the same opportunity to seek suppression of evidence and/or discovery as would any other criminal defendant who received a FISA notice. The plea agreement conveyed benefits to both the government and Hasbajrami. Litigating the legality of the FISA collection now, as Hasbajrami essentially requests, would extinguish the benefits that inured to the government under the terms of the plea. If he wants to engage in such litigation, Hasbajrami must abandon the benefits he derived under the plea agreement.

I. BACKGROUND

As set forth in the Presentence Investigation Report (“PSR”), Hasbajrami’s case arose from an investigation by agents of the Joint Terrorism Task Force (“JTTF”), which revealed that between April 2, 2011 and August 28, 2011 Hasbajrami communicated with a Pakistan-based extremist (“Individual #1”) who informed Hasbajrami that he was part of a terrorist organization. (PSR ¶ 2). Individual #1, a foreign national whose identity is known to the parties, told Hasbajrami that his group was engaged in attacks on American soldiers in Afghanistan. In addition, Individual #1 promoted violent extremist activity through Internet communications and publications, and solicited funds that he represented would be used to support terrorist operations. (Id.)

During the course of their communications, Hasbajrami sent approximately \$1,000 to Individual #1 to support Islamic fundamentalist terrorist operations. In addition, Hasbajrami and Individual #1 planned for Hasbajrami’s travel from New York to the Federally Administered Tribal Areas (“FATA”) of Pakistan, where Hasbajrami hoped to join a jihadist fighting group. (Id.) During their communications, Hasbajrami discussed with Individual #1 his desire to “marry with the girls in paradise,” that is, to die as a martyr while engaged in fighting a holy war. (Id.)

indictment, which charged him with attempting to provide material support to terrorists in violation of 18 U.S.C. § 2339A(a). The plea agreement expressly provided: “The defendant agrees not to file an appeal or otherwise challenge, by petition pursuant to 28 U.S.C. § 2255 or any other provision, the conviction or sentence in the event that the Court imposes a term of imprisonment of 15 years or below. . . . The defendant waives any right to additional disclosure from the government in connection with the guilty plea.” (Plea Agr. ¶ 4).

In his allocution, Hasbajrami stated:

Between April 1, 2011 and September 6, 2011, I tried to help a group of people who I believed were engaged in fighting in Pakistan. I agreed with the group and attempted to help the group by providing money, and myself, in support of their efforts. I obtained an Iranian visa and, on September 6, 2011, I went to JFK in Queens, New York in an effort to travel to Middle East in an effort to join the group.

(Plea Tr. 18-19). Thus, there is no question as to Hasbajrami’s factual guilt. At the plea proceeding, the Court confirmed Hasbajrami’s understanding that he was waiving his right to challenge his conviction or sentence:

THE COURT: In your bargain with the government, you’ve given up your right to otherwise appeal any sentence or conviction, or challenge it in any other way, not just by appeal but by any legal way, as long as you don’t get more than 15 years in jail, understood?

HASBAJRAMI: Okay.

(Plea Tr. 15). At sentencing on January 8, 2013, the Court accepted the plea and imposed a sentence of 15 years’ imprisonment, noting that the Court may well have imposed a higher sentence but for the statutory maximum. (Sent. Tr. 34) (The Court remarked, “I think in order to accurately reflect the seriousness of your conduct, a sentence would be greater than 15 years in jail. What you did is that serious a crime, that worthy of condemnation.”). At the conclusion of sentencing, the government moved to dismiss the open counts, as it was obligated to do by the

II. APPLICABLE LAW

While Hasbajrami's pending motion purports to be a motion for discovery, it implicates several important areas of substantive law relating to the authority by which the government may obtain foreign intelligence information and use FISA and FAA Section 702 obtained or derived evidence, as well as the propriety of the government's conduct in this and other national security cases. Notably, many of the defendant's same claims were very recently addressed and rejected by the district court in United States v. Mohamud, , Cr. No. 3:10-00475 (KI) 2014 WL 2866749 (D. Or. June 24, 2014). Mohamud is directly on point, for example, as to Hasbajrami's various claims about the purported existence of "secret" government notice policies as well as the constitutionality of Section 702, and is a well-reasoned decision worthy of this Court's consideration in its entirety.²

In addition to the analysis set forth in Mohamud, the basic principles and authorities that relate to the instant motion are summarized below, and discussed in greater detail in the context of Hasbajrami's specific arguments.

² Because Mohamud involved the provision of Section 702 notice after trial, but before sentencing, the district court also addressed the availability of FISA's suppression remedy in such circumstances. In Mohamud, the district court recognized that, when enacting the FISA statute, Congress opted to provide the single remedy of suppression when the government unlawfully acquires evidence under the statute, and held that suppression is also the sole remedy when notice is untimely. Mohamud, 2014 WL 2866749 at *3. The district court also recognized that FISA "even anticipates a suppression motion may be filed after trial: 'Such a motion shall be made before the trial . . . unless . . . the person was not aware of the grounds of the motion.'" Id. (citing 50 U.S.C. § 1806(c)). While Fourth Amendment claims for suppression of evidence are not cognizable in a Section 2255 proceeding as explained herein, Hasbajrami would be able to seek a suppression remedy if his guilty plea were vacated.

A. The Foreign Intelligence Surveillance Act

Foreign intelligence information may be collected pursuant to traditional authority under FISA (e.g. Title I electronic surveillance and Title III physical search), as well as through means authorized by the FISA Amendments Act of 2008, or “FAA.” Section 702 of Title VII of FISA permits the targeting of electronic communications of non-U.S. persons located outside of the United States, subject to certain statutory requirements. 50 U.S.C. § 1881a. Section 702 provides that “upon the issuance” of an order from the Foreign Intelligence Surveillance Court (“FISC”), “the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year . . . the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.” 50 U.S.C. § 1881a(a). Collection under this section is subject to numerous statutory requirements and extensive oversight, including inter alia a finding by the FISC that the procedures governing targeting decisions and the use and dissemination of the information that is obtained are “consistent with the fourth amendment to the Constitution of the United States” and the statute, as well as statutory limitations that are directed at preventing the intentional targeting of U.S. persons or persons located within the United States. 50 U.S.C. § 1881a(b).

Under FISA, the government must notify any “aggrieved person” of its intent to “enter into evidence or otherwise use or disclose,” in a proceeding against such person, “any information obtained or derived from [FISA authorized] electronic surveillance of that aggrieved person.” 50 U.S.C. § 1806(c).³ The FAA provides that “[i]nformation acquired from an

³ Section 1825(d) provides the same notice provision with respect to physical searches conducted pursuant to FISA authority. 50 U.S.C. § 1825(d). An “aggrieved person” is defined as “a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance.” 50 U.S.C. § 1801(k).

acquisition conducted under section 1881a of this title [i.e. Section 702] shall be deemed to be information acquired from an electronic surveillance pursuant to subchapter I of this chapter [i.e. Title I] for purposes of section 1806 [FISA’s notice provision]. . .” 50 U.S.C. § 1881e(a). FISA further provides that an “aggrieved person” may move to suppress evidence obtained or derived from FISA-authorized surveillance on the ground that it was “unlawfully acquired” or “the surveillance was not made in conformity with an order of authorization or approval.” 50 U.S.C. §1806(e). Any such motion must be filed in advance of the proceeding in which it will be used, “unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.” Id. If a suppression motion is filed, a district court “shall . . . review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary” if the Attorney General certifies that an adversary hearing would harm national security. 50 U.S.C. 1806(f). If the district court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure. Id.

B. Collateral Proceedings under 28 U.S.C. § 2255

1. A Section 2255 Petitioner Must Show That The Discovery He Seeks Would Establish a Legal Claim That Would Entitle Him To Relief

Prisoners who collaterally attack their federal convictions under 28 U.S.C. § 2255 are “not entitled to discovery as a matter of ordinary course.” Bracy v. Gramley, 520 U.S. 899, 904 (1997). Instead, under Rule 6(a) of the Rules Governing Section 2255 Proceedings, a district judge may authorize a party to conduct discovery only for “good cause.” The Supreme Court has interpreted that term to mean “specific allegations before the court [that] show reason to believe that the petitioner may, if the facts are fully developed, be able to demonstrate that he is . . . entitled to relief.” Id. at 908-09 (quoting Harris v. Nelson, 394 U.S. 286, 300 (1969)).

Moreover, as courts of appeals have repeatedly recognized, Rule 6(a) neither “authorize[s] fishing expeditions” nor allows discovery on the basis of “conclusory allegations,” but instead requires specific allegations that, if developed, would entitle the petitioner to relief on a specific legal claim. Harris v. Johnson, 81 F.3d 535, 540 (5th Cir.1996); see also Hubanks v. Frank, 392 F.3d 926, 933-34 (7th Cir. 2004) (good cause for discovery “cannot exist where the facts alleged do not provide a basis for relief”); Stanford v. Parker, 266 F.3d 442, 460 (6th Cir. 2001) (no error in denial of “a fishing expedition masquerading as discovery” motion); Hill v. Johnson, 210 F.3d 481, 487-88 (5th Cir. 2000) (petitioner must establish “a prima facie [case] for relief” supported by allegations that must be “specific, as opposed to merely speculative or conclusory, to justify discovery”); Murphy v. Johnson, 205 F.3d 809, 814 (5th Cir. 2000) (discovery on Brady claim properly denied where petitioner made only conclusory or speculative allegations, as opposed to a prima facie showing that undisclosed exculpatory information existed or that it was material to the outcome of the case); Clark v. Johnson, 202 F.3d 760, 767 (5th Cir. 2000) (motion for discovery to investigate “hidden” facts underlying claim for relief was “tantamount to a request for an impermissible fishing expedition”); Rich v. Calderon, 187 F.3d 1064, 1067-68 (9th Cir. 1999) (denying discovery where petitioner failed to identify specific claims that might entitle him to relief, because discovery under Rule 6 “was never meant to be a fishing expedition for habeas petitioners to ‘explore their case in search of its existence’”); Deputy v. Taylor, 19 F.3d 1485, 1492-93 (3rd Cir.1994). Thus, to establish good cause for discovery, a petitioner must “identify the essential elements of [his] substantive claim” and make a specific and concrete prima facie showing that, if discovery were allowed, he could satisfy each element of his claim for relief and defeat any procedural bars that would prevent the court from reaching the merits of his claim. Newton v. Kemna, 354 F.3d 776, 783-84 (8th Cir. 2004) (internal quotation marks and citation

Similarly, a defendant may be entitled to withdraw his guilty plea where the government has engaged in misconduct. United States v. Fisher, 711 F.3d 460, 465-66 (4th Cir. 2013).

Here, as discussed further below, Hasbajrami has not moved to vacate his guilty plea, but rather made a broad and speculative discovery demand relating to the legal authorities and facts underlying the investigation of his criminal conduct.

C. Discovery Standards

In the course of a criminal case, the government is obligated to produce information pursuant to four basic categories of discovery: (1) the materials described in Rule 16 of the Federal Rules of Criminal Procedure; (2) prior statements of a witness, pursuant to 18 U.S.C. § 3500; (3) impeachment material pursuant to Giglio v. United States, 405 U.S. 150 (1972), in cases which proceed to trial; and (4) exculpatory evidence as defined by Brady v. Maryland, 373 U.S. 83 (1963), and its progeny. In order to obtain discovery based on a claim of prosecutorial misconduct, a defendant must present a threshold showing of some evidence that the alleged prosecutorial misconduct occurred, to rebut the presumption that prosecutors have acted in good faith. See, e.g., United States v. Armstrong, 517 U.S. 456, 464, 468-69 (1996) (holding that, because “courts presume that [prosecutors] have properly discharged their official duties,” defendants seeking discovery in support of a selective prosecution claim must make a “threshold showing”); see also United States v. Arenas-Ortiz, 339 F.3d 1066, 1069 (9th Cir. 2003) (describing Armstrong standard as “rigorous”).

In addition where, as here, discovery demands implicate classified materials relating to FISA and Section 702 materials, there are specific statutory conditions that directly govern production of those materials, the unauthorized disclosure of which could cause grave harm to national security. See 50 U.S.C. §§ 1806(f) and 1881e(a). The Court can only order disclosure of any portion of the Section 702 materials submitted for in camera, ex parte review if

the Court has first concluded that it is unable to make an accurate determination of the legality of the collection by reviewing the government's submissions (and any supplemental materials that the Court may request). *Id.* If the Court is able to accurately determine the legality of the collection based on its *in camera*, *ex parte* review of the materials the government submits, then the FISA statute prohibits disclosure of any of those materials to the defense, unless otherwise required by due process. *See, e.g., United States v. El-Mezain*, 664 F.3d 467, 566 (5th Cir. 2011); *United States v. Duggan*, 743 F.2d 59, 78 (2d Cir. 1984).

ARGUMENT

I. HASBAJRAMI HAS NO RIGHT TO DISCOVERY ON COLLATERAL ATTACK

Hasbajrami's criminal case is closed. He does, however, have a pending motion under Section 2255, and the government has not objected to him amending that pending petition to address the Supplemental Notification. Prisoners such as Hasbajrami who collaterally attack their federal convictions under 28 U.S.C. § 2255, however, are "not entitled to discovery as a matter of ordinary course." *Bracy*, 520 U.S. at 904. For the reasons set forth below, he is precluded from obtaining the discovery he seeks in this civil Section 2255 proceeding.⁴

Hasbajrami's motion seeks broad discovery over a wide range of issues, including internal government deliberations regarding the provision of the original FISA notice and the Supplemental Notification, and the legality of the Title VII collection from which certain of the evidence the government intended to use at trial was derived. Hasbajrami ignores, however, the applicable standard for obtaining discovery in the context of a collateral proceeding under 28 U.S.C. § 2255. Under that standard, a petitioner may only obtain discovery if he sets forth

⁴ Indeed, even if he were successful in vacating his guilty plea and reopening his case, he would not be entitled to the discovery he seeks.

specific factual allegations that, if fully developed through discovery, would support a particular legal claim that would entitle him to relief in the collateral proceeding.

As discussed in greater detail below, Hasbajrami's motion does not satisfy that standard. He has not yet raised any substantive claim related to the Section 702 collection. Although he contends that discovery is warranted to support various constitutional and statutory challenges to the legality of the Section 702 collection that he may raise in a future amendment to his Section 2255 motion, Hasbajrami is foreclosed in this collateral proceeding from bringing any of the claims he identifies other than a challenge to the voluntariness of the plea. And, as explained below, none of the discovery Hasbajrami seeks is relevant to that claim.

A. Hasbajrami has not raised a substantive claim.

The primary habeas claim pending before this Court is Hasbajrami's challenge to the constitutionality of 18 U.S.C. § 2339A, an issue unrelated to the nature and legality of the collection of the evidence that would have been used to prove his guilt of that crime in the criminal case. Although the motion for discovery is premised on the proposition that Hasbajrami might decide to seek to withdraw his guilty plea, he has not made such a claim. For this reason alone, Hasbajrami is not entitled to any discovery. See Puglisi v. United States, 586 F.3d 209, 213 (2d Cir. 2009) ("There is no pre-motion discovery in a Section 2255 case"). Hasbajrami claims entitlement to discovery in order to assess the potential merits of such a claim, but he cites no authority in which a court has granted discovery before the moving party has actually asserted the claim to which the discovery purportedly relates.⁵ When a defendant faces a decision whether to plead guilty (or to challenge a plea he has already entered), he must always do so in the face of uncertainty about whether that decision will result in a better or worse outcome than if he refused

⁵ Indeed, the fact that he has not moved to withdraw his plea is a strong indication that he has suffered no prejudice whatsoever from the timing of the Supplemental Notification.

involuntary. For that reason, Hasbajrami cannot establish “good cause” for discovery.⁶

1. Hasbajrami’s Guilty Plea Forecloses His Constitutional and Statutory Challenges to the Legality of the Section 702 Collection

Hasbajrami suggests that he intends to challenge Section 702 collection in his case on the ground that it violated the Fourth Amendment, other constitutional provisions, and the applicable statutory requirements. (See, e.g., Def. Mot. at 3, 10, 30). Those claims are foreclosed, however, by Hasbajrami’s unconditional guilty plea. As the Supreme Court has observed, a guilty plea constitutes “a break in the chain of events which has preceded it in the criminal process.” Tollett, 411 U.S. at 267. Accordingly, “[w]hen a criminal defendant has solemnly admitted in open court that he is in fact guilty of the offense with which he is charged, he may not thereafter raise independent claims relating to the deprivation of constitutional rights that occurred prior to the entry of the guilty plea.” Id. Rather, a defendant seeking to raise such “antecedent constitutional violations,” id. at 266, is limited to attacks on the knowing, voluntary, and intelligent character of the guilty plea. United States v. Broce, 488 U.S. 563, 569 (1989). As the Supreme Court has explained,

A plea of guilty and the ensuing conviction comprehend all of the factual and legal elements necessary to sustain a binding, final judgment of guilt and a lawful sentence. Accordingly, when the judgment of conviction upon a guilty plea has become final and the offender seeks to reopen the proceeding, the inquiry is ordinarily confined to whether the underlying plea was both counseled and voluntary. If the answer is in the affirmative then the conviction and the plea, as a general rule, foreclose the collateral attack.

⁶ Even if, despite his guilty plea, Hasbajrami could somehow directly challenge the lawfulness of the Section 702 collection in this collateral proceeding, his claims would be foreclosed by a number of procedural bars, including the general bar on collateral review of Fourth Amendment claims, see Stone v. Powell, 428 U.S. 465, 494 (1976), the bar on retroactive application of new procedural rules, see Teague v. Lane, 489 U.S. 288, 308 (1989), and the bar on collateral relief based on non-constitutional errors, see Graziano v. United States, 83 F.3d 587, 589-90 (2d Cir. 1996). Because these procedural bars would prevent the court from reaching the merits of his claims, Hasbajrami cannot establish “good cause” for discovery. See Newton, 354 F.3d at 783-84.

Id.

Under these principles, Hasbajrami's guilty plea bars him from raising claims that his conviction was based on evidence obtained in violation of the Fourth Amendment or other constitutional or statutory provisions. See Haring v. Prosise, 462 U.S. 306, 320-22 (1983) (stating that, after a defendant pleads guilty, his conviction does not rest on the evidence that he claims was improperly seized and therefore it "cannot be affected by an alleged Fourth Amendment violation"); United States v. Arango, 966 F.2d 64, 66 (2d Cir. 1992) (defendant who pled guilty waived claim that search of his van violated Fourth Amendment); United States v. Sykes, 697 F.2d 87, 89 (2d Cir. 1983) (guilty plea waived challenge to search warrant); United States v. Selby, 476 F.2d 965, 966-67 (2d Cir. 1973) (guilty plea waived appeal of motion to suppress documentary evidence); Smith v. United States, 876 F.2d 655, 657 (8th Cir. 1989) (defendant's guilty plea "waived his claims on search and seizure"). Accordingly, Hasbajrami may not bring any such claims in this collateral proceeding. Hasbajrami may only challenge the legality of the surveillance if he obtains collateral relief on a challenge to the voluntariness of his guilty plea and, following any appeals, the criminal case is reopened and he files a motion to suppress FAA-derived evidence. But Hasbajrami may not obtain discovery now to support a claim that he may be able to bring at some future time; rather, he is only entitled to discovery to support claims that would entitle him to relief in this collateral proceeding. For that reason, Hasbajrami cannot establish good cause for discovery on the ground that it would be helpful in challenging the lawfulness of the Section 702 collection.

Moreover, Hasbajrami also is barred from bringing a constitutional or statutory challenge to the Section 702 collection because Hasbajrami's plea agreement expressly provided that, "The defendant agrees not to file an appeal or otherwise challenge, by petition

defendant might labor”).

In sum, any Fourth Amendment or other challenges to the legality of the Section 702 collection that Hasbajrami may attempt to raise are doubly waived. First, Hasbajrami’s unconditional guilty plea forecloses claims asserting constitutional or statutory violations that occurred prior to the entry of the plea. Second, Hasbajrami is barred from challenging the lawfulness of the collection because he agreed in his plea agreement not to challenge his conviction on any basis other than that his sentence exceeded the 15-year statutory maximum.

2. The Discovery Hasbajrami Seeks Relating to the Supplemental Notification Does Not Implicate the Validity of his Plea

Hasbajrami’s motion also seeks discovery to support a potential challenge to his plea on the ground that the government’s failure to provide specific notice of intent to use Section 702-derived information at trial rendered his guilty plea involuntary. Unlike the other potential claims Hasbajrami identifies, that claim is not foreclosed by Hasbajrami’s guilty plea. However, the discovery Hasbajrami now seeks would not assist him in attempting to establish that his plea was involuntary, and for that reason, his motion must fail.

The fact that Hasbajrami may not have been specifically aware of, and did not specifically waive, potential claims related to Title VII surveillance does not undermine the knowing and voluntary nature of his plea. See Broce, 488 U.S. at 573 (“Our decisions have not suggested that conscious waiver is necessary with respect to each potential defense relinquished by a plea of guilty.”); Ricketts v. Adamson, 483 U.S. 1, 9-10 (1987) (explaining that the Court did “not find it significant” that a double-jeopardy claim “was not specifically waived by name in the plea agreement”); United States v. Leyland, 277 F.3d 628, 631-32 (2d Cir. 2002) (conscious relinquishment of the particular claim is not required). Rather, contrary to Hasbajrami’s

contention, a guilty plea extinguishes constitutional defenses of which the defendant may have no knowledge. In Broce, the Supreme Court noted that “[o]ur decisions have not suggested that conscious waiver is necessary with respect to each potential defense relinquished by a plea of guilty” because relinquishment “derives not from any inquiry into a defendant’s subjective understanding of the range of potential defenses, but from the admissions necessarily made upon entry of a voluntary plea of guilty.” 488 U.S. at 573-74. The Court then held that the plea in that case had relinquished a potential defense under the Double Jeopardy Clause of which the defendant had no knowledge. Id. at 572-74; see also Ruiz, 536 U.S. at 629-30 (observing that “the law ordinarily considers a waiver knowing, intelligent, and sufficiently aware if the defendant fully understands the nature of the right and how it would likely apply in general in the circumstances -- even though the defendant may not know the specific detailed consequences of invoking it.”).⁷ Hasbajrami cites no cases suggesting that a guilty plea is invalid where the defendant is not informed of the specific legal authority governing surveillance whose fruits the government intended to introduce.

To be sure, in extraordinary circumstances where the defendant has been induced to

⁷ In addition, under analogous circumstances, the Fifth Circuit has held that the government’s failure to disclose the legal process by which it obtained evidence does not constitute a discovery violation that would render a defendant’s plea invalid. See United States v. McLean, 419 Fed. Appx. 473, 474 (5th Cir. 2011) (rejecting appellant’s argument that “the district court erred by not allowing him to withdraw his guilty plea based on the Government’s undisclosed discovery when the discovery would have likely resulted in suppression based on the Government’s improper use of an administrative summons to obtain his internet subscriber records”). In McLean, the appellant argued that, but for the nondisclosure of a summons, he would not have entered a plea. In its unpublished decision, the Fifth Circuit held that “McLean’s guilty plea precludes him from claiming that the Government’s alleged failure to disclose the summons was a Brady violation, or from claiming that the use of the summons was unconstitutional. We conclude that McLean’s guilty plea was knowing and voluntary, as did the district court.” Id. (citations omitted). Similarly, here, Hasbajrami’s guilty plea precludes him from raising a Fourth Amendment challenge.

plead guilty by egregious misrepresentations or other serious misconduct, a court may find that the defendant was deprived of his ability to plead guilty voluntarily. See Bousley v. United States, 523 U.S. 614, 619 (1998) (a plea entered by defendant with awareness of the consequences is voluntary unless it is induced by threats or misrepresentation). To have his plea vacated, however, the defendant must show that his decision to plead guilty was induced by a misrepresentation that “strikes at the integrity of the prosecution as a whole,” and he must establish a reasonable probability that, but for the misrepresentation, he would not have pleaded guilty. See Fisher, 711 F.3d at 466 (concluding on collateral review that guilty plea was rendered involuntary because police officer fabricated facts in application for a search warrant and defendant would have moved to suppress, rather than pleading guilty, had he known of the misrepresentations).⁸

Here, Hasbajrami cannot establish that there is “reason to believe” that, if his discovery motion is granted, he would “be able to demonstrate that he is . . . entitled to relief” on this ground. Bracy, 520 U.S. at 908-909. First, as explained more fully below, there is no indication that the government’s post-conviction filing of the Supplemental Notification reflects any bad faith or willful misconduct, much less an affirmative misrepresentation that undermines the integrity of the prosecution as a whole. Indeed, in Mohamud, as the district court recently explained in a case where the government provided supplemental notification after the defendant was convicted at trial:

⁸ Any challenge to the voluntariness of Hasbajrami’s plea was forfeited and therefore subject to a cause and prejudice standard. Bousley, 523 U.S. at 621 (“[T]he voluntariness and intelligence of a guilty plea can be attacked on collateral review only if first challenged on direct review.”). Even if the post-conviction Supplemental Notification satisfies the “cause” prong, Hasbajrami must still establish “actual prejudice.” In the guilty plea context, “actual prejudice” requires that he establish, at a minimum, a reasonable probability that he would not have pleaded guilty. The discovery that he seeks is not relevant to that inquiry.

Clearly a lot of time has passed, but otherwise suppression and a new trial would put defendant in the same position he would have been in if the government notified him of the § 702 surveillance at the start of the case. Moreover, the government has apparently changed its practice in making this type of notification, so dismissal is not needed as a deterrence.

In addition, once the government changed its legal opinion about when evidence could be derived under Title VII, it performed the second review of this case and provided the Supplemental Notification without prodding from the court or the defense. If the government had kept mum about the situation in this case, I would have sentenced defendant months ago. I consider this strong evidence of the lack of prosecutorial misconduct.

Mohamud, 2014 WL 2866749, at* 4; see also United States v. Gale, 314 F.3d 1, 6 (D.C. Cir. 2003) (discovery not warranted where there is “no real chance that discovery could have turned up information altering the outcome”).

Moreover, the voluntariness of Hasbajrami’s plea does not depend on the government’s internal deliberations or on the specific details of the Section 702 collection because Hasbajrami, at the time of his plea, would have had the same (or less) information on those topics that he possesses now. In other words, the key issues in Hasbajrami’s potential voluntariness challenge -- whether the absence of Section 702 notice was so fundamental as to undermine Hasbajrami’s ability to enter a valid plea and whether, had he received notice, he would have insisted on going to trial -- must be based on the information that was or should have been available to Hasbajrami at the time of the plea. In addition, by virtue of the ex parte review provisions of the FISA statute, a pre-plea motion to suppress by Hasbajrami would similarly have been made without the benefit of the “discovery” he now seeks. 50 U.S.C. § 1806(f).

If, at the time of the plea discussion, Hasbajrami had insisted on seeking discovery related to Section 702 surveillance before pleading guilty, there would have been no plea agreement. As the government explained to the Court prior to sentencing pursuant to Rule

11(c)(3)(A) and Section 6B1.2 of the United States Sentencing Guidelines, the government offered Hasbajrami a plea agreement that substantially reduced Hasbajrami's sentencing exposure and one of the benefits that the government received was avoiding the costs and risks of litigation related to the FISA collection (See ECF No. 39). Accordingly, the discovery Hasbajrami now seeks has no bearing on whether he would have accepted the government's offer if Title VII notice had been provided, because he would have had to make his decision based on the same information that he possesses now.

II. HASBAJRAMI CANNOT JUSTIFY DISCLOSURE OF THE REQUESTED MATERIALS ON ANY OTHER BASIS

A. Hasbajrami fails to establish government misconduct.

As discussed in greater detail below, Hasbajrami argues that he is entitled to discovery regarding the circumstances surrounding the government's filing of the Supplemental Notification, alleging that it was a "deliberate violation of the notice statute" (Def.'s Mot. at 10); that it "resulted from knowing and intentional misconduct by Government actors" (id.); and that the government has engaged in a "secret policy" intended to withhold information from defense counsel nation-wide. (Id. at 18). Hasbajrami also erroneously claims that the sequence of events surrounding the filing of the Supplemental Notice in this case and two others, United States v. Muhtorov, 12 Cr. 33 (JLK) (D. Colo.) (ECF No. 457), and United States v. Mohamud, 10 Cr. 457 (KI) (D. Or.) (ECF No. 486), demonstrates an intentional, systemic violation of the FISA notice provision by the government. (Id. at 15-22). It does not.

In addition, Hasbajrami incorrectly informs the Court that the government has given Supplemental Notice of FAA-derived information in only three cases, alleging that the government conspiratorially chose three cases in different procedural postures to serve as "test cases." (Id. at 20). In fact, the government has publicly provided supplemental Section 702

notice in five cases to date. In addition to the three cases cited by Hasbajrami, the government has provided supplemental notice in United States v. Oytun Mihalik, 11 Cr. 00833 (JLS) (C.D.C.A.) (ECF No. 145) (also a post-plea supplemental notice regarding Section 702, in the identical posture to this case, which the defendant has not challenged), and United States v. Reaz Khan, 3:12 Cr. 00659 (MO) (D. Or.) (ECF No. 59) (trial pending).

Moreover, while Hasbajrami relies on the government's notice in Mohamud, he fails to inform the Court that in that case, where the government provided supplemental notice post-trial, the district court denied a nearly identical discovery motion, seeking nearly identical materials, and advancing nearly identical arguments as those asserted here. Mohamud, 10 Cr. 457 (KI) (D. Or.) (ECF No. 499). Also, as noted above, on June 24, 2014, the Oregon district court issued a lengthy written opinion and order denying the defendant's motion to vacate the conviction, dismiss the indictment, suppress evidence, and grant a new trial for the government's "violation" of the pretrial notice statute.⁹ See Mohamud, 2014 WL 2866749. In Mohamud, a jury convicted the defendant in January 2013 of attempting to use a weapon of mass destruction, in violation of 18 U.S.C. § 2332a(a)(2)(A). The government filed a supplemental FISA notification, very similar to the one in this case, on November 19, 2013. Of note, in denying the defendant's post trial motion to vacate his conviction, the district court found Section 702 constitutional as applied in that case. Id.

B. The timing of the Supplemental Notification is not indicative of bad faith.

At the outset, Hasbajrami's claim that the government engaged in deliberate misconduct to conceal the use of Title VII-derived evidence is unfounded. The Department has

⁹ In that same opinion and order, the district court also denied the defendant's alternative motions for suppression of evidence and a new trial based on the government's alleged introduction at trial (and other uses) of information derived from unlawful surveillance, and the defendant's second motion for a new trial. Mohamud, 2014 WL 2866749, at *5.

always understood that it is required to notify any “aggrieved person” of its intent to use or disclose, in a proceeding against such person, any information obtained or derived from Title VII collection, in accordance with 50 U.S.C. §§ 1806(e), 1881e(a). The Department’s determination, however, that information obtained or derived from Title I or Title III collection may, in particular cases, also be derived from prior Title VII collection is a relatively recent development (and one that occurred after Hasbajrami pleaded guilty). The timing of the Supplemental Notification was far from ideal, but it is not indicative of bad faith. The Supplemental Notification filed in this case, which the government provided based on its own review, resulted from the Department’s determination and demonstrates good faith, not misconduct.

The Department has always understood that notice pursuant to Sections 1806(c), 1825(d) and 1881e(a) must be provided when the government intends to use evidence directly collected pursuant to Title I, III, or VII. Such evidence would be evidence that was “obtained from” such FISA collection. Likewise, the Department has always recognized that notice pursuant to those provisions must be provided when the government intends to use evidence obtained through ordinary criminal process (such as a Rule 41 search warrant) that was itself based directly on information obtained pursuant to Title I, III, or VII. Such evidence clearly would be evidence that was “derived from” such FISA collection.

Until last year, however, the Department had not considered the particular question of whether and under what circumstances information obtained through electronic surveillance under Title I or physical search under Title III could also be considered to be derived from prior collection under Title VII. After conducting a review of the issue, the Department determined that information obtained or derived from Title I or Title III FISA collection may, in particular cases, also be derived from prior Title VII collection, such that notice concerning both Title I/III

and Title VII collections should be given in appropriate cases with respect to the same information.¹⁰

In the matter at hand, in September 2011, at the time the original FISA notice was filed in this case, the government was aware of the fact that some of the evidence to be used had been obtained or derived from Title I and Title III FISA collection. Indeed, prior to Hasbajrami's plea, the government produced in discovery the evidence on which it intended to rely, including declassified email communications, some of which evidence and information had been obtained pursuant to FISA. The government did not determine, prior to the plea or sentencing in this case, whether that same evidence also was "derived," as a matter of law, from prior FISA collection pursuant to Title VII. Based on the Department's recent determination, which occurred long after Hasbajrami pleaded guilty and was sentenced, the government reviewed the evidence that it had produced in discovery and would have offered against Hasbajrami at trial had he not pleaded guilty, and determined that some of the evidence obtained and derived from Title I and Title III collection was also derived from Section 702 collection as a matter of law. As a result, the government provided the Supplemental Notification, in an abundance of caution, to inform Hasbajrami and the Court that the government had intended to offer into evidence or otherwise use Section 702-derived information to prove the defendant's guilt had the case proceeded to trial.

In this case, the government acted in accordance with the Department's then-current standard practice and under a good faith understanding that the initial notice of the use of Title I and Title III FISA evidence fully satisfied the government's notice obligations.

¹⁰ The Department has concluded that in determining whether information is "obtained or derived from" FISA-authorized surveillance, the appropriate standards and analyses are similar to those appropriate in the context of surveillance conducted pursuant to Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-2522.

obtain discovery based on a claim of prosecutorial misconduct, a defendant must present a threshold showing of some evidence that the alleged prosecutorial misconduct occurred to rebut the required presumption that prosecutors have acted in good faith. See, e.g., Armstrong, 517 U.S. at-464, 469 (holding that, because “courts presume that [prosecutors] have properly discharged their official duties,” defendants seeking discovery in support of a selective prosecution claim must make a “threshold showing”); United States v. Arenas-Ortiz, 339 F.3d 1066, 1069 (9th Cir. 2003) (describing Armstrong standard as “rigorous”). Hasbajrami has not made such a showing in this case. Although the government does not dispute that the notice was untimely, Hasbajrami has not otherwise produced evidence to overcome the presumption that the government in this case acted in good faith.

While the government understands that it is solely responsible for the untimeliness of the notice in this case, the post-plea filing of the Supplemental Notification does not reflect any bad faith or willful misconduct, and it does not call into question the defendant’s factual guilt. Rather, it is the result of a careful review of the range of circumstances in which information obtained or derived from Title I or Title III collection should also be considered as a matter of law to be derived from prior Title VII collection, such that the government should give notice of both Title I/III and Title VII surveillance in those cases. This type of internal review and implementation of remedial measures is not indicative of misconduct. See Mohamud, 2014 WL 2866749, at *4 (noting the Department’s recent determination and finding “strong evidence of the lack of prosecutorial misconduct” under the circumstances).

A. Late notice does not constitute a Brady violation.

Hasbajrami raises the specter of a Brady violation based on the timing of the Supplemental Notification. (See, e.g., Def. Mot. at 24 (stating that, “In the context of a guilty

plea, undisclosed exculpatory information is material when ‘there is a reasonable probability that but for the failure to produce such information the defendant would not have entered the plea but instead would have insisted on going to trial’) (citing Tate v. Wood, 963 F.2d 20, 24 (2d Cir. 1992)). The district court in Mohamud rejected a similar claim and the government urges this Court to do so as well. Mohamud, 2014 WL 2866749, at *6. As Hasbajrami correctly recognizes, “Brady requires that the government disclose material evidence favorable to a criminal defendant.” United States v. Mahaffy, 693 F.3d 113, 127 (2d Cir. 2012). Yet, Hasbajrami points to no case, and the government is not aware of any, in which the late notice of the legal authority underlying the collection of evidence constituted a Brady violation – particularly where, as here, that legal authority has expressly been held to be lawful under similar circumstances. See Mohamud, 2014 WL 2866749, at *27 (“Based on the statutory protections, I conclude the government’s compelling interest in protecting national security outweighs the intrusion of § 702 surveillance on an individual’s privacy. Accordingly, § 702, as applied to defendant, is reasonable under the Fourth Amendment.”); see also In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004 (FISC Ct. Rev. 2008) (upholding the constitutionality of the Protect America Act, which was the predecessor to the FAA and granted a broader authority under which the DNI and Attorney General could jointly authorize the acquisition of foreign intelligence information concerning persons reasonably believed to be located outside the United States).

As the Supreme Court has explained, “There are three components of a true Brady violation: The evidence at issue must be favorable to the accused, either because it is exculpatory, or because it is impeaching; that evidence must have been suppressed by the State, either willfully or inadvertently; and prejudice must have ensued.” Strickler v. Greene, 527 U.S. 263, 281-82

the offense for which he pleaded guilty, are material in the relevant sense.¹¹ As one district court in this Circuit has observed, “the fact that the color of the traffic light would be relevant [in a motor vehicle incident] would not justify disclosure of what a motorist told his or her lawyer on that subject. So too here. The fact that the reasons for delay in this case are pertinent does not justify disclosure of privileged communications arguably pertinent to that subject because there has been no reliance by the government on those communications.” Ghailani, 751 F. Supp. 2d at 502.

Hasbajrami’s reliance on United States v. Reynolds, 345 U.S. 1, 12 (1953), for the proposition that the government cannot invoke governmental privileges to “deprive the accused of anything which might be material to his defense” is also misplaced. Here, the government complied with all of its Brady obligations before Hasbajrami entered his plea. Indeed, as noted above, the government disclosed classified information to cleared defense counsel prior to the plea in the context of negotiating a fair resolution. (See ECF No. 28). The government’s internal discussions surrounding the provision of the Supplemental Notification are not material to his instant petition or to his defense had he gone to trial because the Supplemental Notification has placed Hasbajrami in the same posture as he would have been in before entering his plea. Hasbajrami has made no cognizable claim as to why he should receive internal documents to which he would not have been entitled prior to the entry of his plea, or had he proceeded to trial. As discussed above, the Supplemental Notification does not amount to new evidence. It was a

¹¹ Hasbajrami’s argument that discovery of internal deliberative documents is not protected by privilege because, according to media reports “several Obama administration officials familiar with the deliberations have already made selective disclosures to the press on the subject,” is similarly meritless. (Def.’s Mot. at 27.) Aside from the question of whether unsourced media reports amount to a privilege waiver by the Department, such records are irrelevant to the only proper questions before this Court in Hasbajrami’s current Section 2255 petition or any future petition relating to his guilty plea. Nor would discovery of internal deliberative documents regarding the provision of notice be appropriate even if the Court eventually set aside Hasbajrami’s plea, undertook motion practice and ultimately ruled against the government on the merits of a suppression motion.

notice that some of the evidence that the government intended to use against Hasbajrami had itself been derived from an additional, lawful surveillance authority, as set forth in Section 702.

Indeed, had Hasbajrami moved to suppress the evidence obtained from FISA-authorized collection based on the original notice in this case, the FISA applications, orders and related materials under which the evidence was obtained or derived would have been presented to the Court in camera and ex parte, as is appropriate under Section 1806(f). Tellingly, early in Hasbajrami's seventy-four page motion is the concession that Hasbajrami is unsure as to whether he even now wishes to seek to vacate his conviction and sentence based on the Supplemental Notification. (Def. Mot. at 5). Hasbajrami is unsure because he understands that he derived a substantial, and not inequitable, benefit from the plea. His motion is, at best, a fishing expedition that casts a wide net, hoping to find something that may support his vague allegation of misconduct and impropriety in the government's national security surveillance programs sufficient to vacate his indictment outright. Hasbajrami should not be permitted to have his cake and eat it too. In his plea agreement Hasbajrami agreed to forgo precisely such an attack.

IV. THERE IS NO BASIS TO ORDER DISCOVERY OF CLASSIFIED MATERIALS RELATING TO THE AUTHORIZATION OR EXECUTION OF SECTION 702 COLLECTION BECAUSE THE LAWFULNESS OF THE COLLECTION IS NOT BEFORE THE COURT

Hasbajrami argues that the Court should grant discovery of the classified materials related to the authorization of the Section 702 collection itself (including the targeting, scope, manner, and authorizations related to the collection), claiming that "there is no question that the defense will challenge the constitutionality of the FAA as part of the substantive motions following completion of discovery." (Def.'s Mot. at 30-36). However, Hasbajrami's putative future challenge to the constitutionality of Section 702 collection provides no basis for discovery of the requested materials and he advances no meaningful argument supporting why he would

require, or be lawfully entitled to such materials to make such a claim. Discovery of FISA-related materials, including that of information regarding any acquisition of foreign intelligence information conducted pursuant to Section 702 of Title VII, is expressly proscribed by the procedures outlined in 50 U.S.C. § 1806(f).¹²

Section 1806(f) requires district courts to conduct an in camera and ex parte review of any materials related to Section 702 collection upon the Attorney General's filing of a declaration stating that disclosure of such materials or an adversary hearing would harm the national security of the United States. 50 U.S.C. §§ 1806(f) and 1881e(a). In turn, a court can only order disclosure of any portion of the Section 702 materials submitted for in camera, ex parte review if the court has first concluded that it is unable to make an accurate determination of the legality of the collection by reviewing the government's submissions (and any supplemental materials that the court may request). Id. If the court is able to accurately determine the legality of the collection based on its in camera, ex parte review of the materials the government submits, then the FISA statute prohibits disclosure of any of those materials to the defense, unless otherwise required by due process. See, e.g., El-Mezain, 664 F.3d at 566; Duggan, 743 F.2d at 78.

Thus, the FISA statute mandates that a district court can order discovery of Section 702-related materials only where the lawfulness of the surveillance itself is at issue, and only where, following its in camera and ex parte review, the court concludes that disclosure to the defense is necessary for it to make an accurate determination of such lawfulness. In the matter at hand, Hasbajrami has not challenged, and cannot challenge, the lawfulness of the Section 702 collection to which he was aggrieved because his plea extinguished that right and such a claim is

¹² 50 U.S.C. § 1881e(a) provides that "information acquired from an acquisition collected under [Section 702] shall be deemed to be information acquired from an electronic surveillance pursuant to [title I]" for purposes of a discovery motion.

not cognizable in a Section 2255 proceeding. Thus, the lawfulness of the collection is not presently before the Court and discovery is unwarranted.

As noted at the outset, Hasbajrami may properly bring a motion for Section 702-related discovery only if his plea is set aside and he proceeds to motion practice and trial. Title 50 U.S.C. § 1806(e) allows a defendant to move to suppress any evidence obtained or derived from collection as to which he is an aggrieved person that will be used against him in a proceeding in the case. This remedy—setting aside the plea and allowing Hasbajrami to file a pre-trial suppression motion—would put Hasbajrami in the same position as if he had received the Supplemental Notification before entering his plea.¹³

Here, Hasbajrami does “not dispute that FISA provides for in camera, ex parte consideration of materials relevant to these motions if certain national security considerations exist” (Def.’s Mot. at 6), but he incorrectly concludes that he can circumvent the FISA discovery process and that this Court can produce FISA-related materials to him now. In support of this contention, Hasbajrami does not cite a single FISA-related district court opinion.

Instead, Hasbajrami improperly relies on language from courts that did not order discovery pursuant to the statutory scheme outlined in FISA, but rather discussed discovery of classified materials under the Classified Information Procedures Act, 18 U.S.C. App. 3 (“CIPA”).

¹³ Because a remedy exists that would fulfil the purpose of FISA’s notice provisions, i.e. to enable defendants to move to suppress, the disclosure that Hasbajrami seeks cannot be necessary to “formulate a remedy” for the provision of late Section 702 notice in this case. (Def.’s Mot. at 23.) There is no need for any additional remedies to deter future government misconduct either. (Id. at 28.) As explained above, there has been no intentional misconduct in this case. And, in any event, the potential for vacatur of guilty pleas and suppression of evidence provides sufficient deterrence of any potential government misconduct. See Davis v. United States, 131 S. Ct. 2419, 2429 (2011) (noting that exclusion of illegally obtained evidence is a “harsh sanction”); United States v. Nicholson, 721 F.3d 1236, 1256 (10th Cir. 2013) (“[E]xclusion is an especially potent remedy” in deterring official misconduct, but “not one individuals may insist on as a matter of personal constitutional right.”) (internal quotation marks and citation omitted).

Although CIPA does govern the use and disclosure in criminal cases of classified information generally, it does not trump or replace the statutory scheme set forth in FISA specified for discovery of materials relating to the authorities set forth in Titles I, III and VII. Thus, Hasbajrami's reliance on United States v. Pappas, 94 F.3d 795, 799-801 (2d Cir 1996) and United States v. Abu Jihaad, 630 F.3d 102, 140 (2d Cir. 2010), is misplaced. CIPA does not apply here -- a civil Section 2255 proceeding involving a motion for discovery of FISA and FAA-related materials. Indeed, in Abu Jihaad, the Second Circuit held that FISA was constitutional as applied and on its face, and that the district court had properly denied the defendant disclosure of FISA related materials and a preliminary hearing to challenge the admissibility of FISA-obtained communications. Id. at 117-130. In addition, in a separate part of the opinion, the circuit court upheld the district court's protective orders issued pursuant to Section 4 of CIPA and the district court's ex parte review of the government's motions for CIPA protective orders. Id. at 139-43.

V. DEFENSE COUNSEL'S SECURITY CLEARANCES ARE NOT A DETERMINATIVE OR LAWFUL BASIS UPON WHICH TO PROVIDE THE REQUESTED DISCOVERY

In addition to conflating CIPA and FISA, Hasbajrami mistakenly asserts that the Court can order the requested discovery because defense counsel possesses the "requisite security clearances." (Def.'s Mot. at 7). This argument is unavailing in both the FISA and CIPA contexts. It is black letter law that the mere possession of a security clearance does not entitle counsel access to classified information. Counsel must also have a "need to know." See Executive Order 13526 §§ 4.1(a) and 6.1 (dd) (requiring that a "need-to-know" determination be made prior to the disclosure of classified information to anyone, including those who possess a security clearance); United States v. Daoud, 755 F.3d 479, 484 (7th Cir. 2014) (finding that district court erred in opining that "any concerns about disclosure [of FISA-related information] were dissolved by the defense counsel's security clearances[,] and noting that it is "a mistake to think

that simple possession of a security clearance automatically entitles its possessor . . . access to classified information that he is cleared to see.”); El-Mezain, 664 F.3d at 568 (“We are unpersuaded by the defendants’ argument that the Government’s interest [in protecting classified information from disclosure to defense counsel] is diminished because defense counsel possess security clearance to review classified material.”); United States v. Amawi, 2009 WL 961143 (N.D. Ohio, Apr. 7, 2009) (cleared counsel denied access to CIPA classified information because they had no need to know); United States v. Abu-Jihaad, 2007 WL 2972623, at *2 (D. Conn. Oct. 11, 2007) (citing United States v. Yousef, 327 F.3d 56, 168 (2d Cir. 2003)); United States v. Libby, 429 F. Supp. 2d 18, 24 n.8 (D.D.C. 2006) (security clearance alone does not justify disclosure because access to classified information is justified only upon a showing that there is a “need-to-know”); accord United States v. Bin Laden, 126 F. Supp. 2d 264, 287 n.27 (S.D.N.Y. 2000); see generally United States v. Ott 827 F.2d 473, 476-77 (9th Cir. 1987) (“Congress has a legitimate interest in authorizing the Attorney General to invoke procedures designed to ensure that sensitive security information is not unnecessarily disseminated to anyone not involved in the surveillance operation in question, whether or not she happens for unrelated reasons to enjoy a security clearance”). Here, Hasbajrami’s discovery motion is not properly before the Court for all of the reasons discussed herein, and, even if it were, defense counsel has no “need to know” under the circumstances and pursuant to Section 1806(f). Respectfully, the matter before the Court is not as “complex” as Hasbajrami asserts (see Def. Mot. at 5). The main issue is simply this: did the government’s failure to notify Hasbajrami of the legal authority underlying the FISA collection before he pleaded guilty render his guilty plea “unknowing” in such a way that undermines the integrity of the prosecution? If so, he should move to vacate his plea and, if successful, proceed to trial. If not, he should enjoy the benefits of his plea bargain, namely a shorter sentence than he

would have received absent the statutory cap that resulted from the plea agreement. In neither instance, however, is defense counsel entitled to sweeping discovery into the inner workings of the government's national security apparatus.

VI. HASBAJRAMI'S SWEEPING ALLEGATIONS RELATING TO GOVERNMENT SURVEILLANCE PROGRAMS ARE NOT GROUNDED IN THE RECORD

Finally, Hasbajrami's vague and sweeping attacks on the secrecy of the government's counter-terrorism efforts are unfounded, speculative and ignore the reality that the government has been able to disrupt and apprehend terrorists, such as Hasbajrami, precisely because its methods are so closely guarded. To the extent that he seeks discovery of the use of other surveillance activities that he speculates may have been used in his case, that request should be denied. None of the other legal authorities or investigative activities raised in his motion is relevant to this case. There is no new evidence in this case, and the Supplemental Notification did not signal otherwise. Moreover, the Supplemental Notification has nothing to do with the "seizure and accessing of internet and telephone metadata" (Def.'s Mot. at 36) or any undisclosed "secret surveillance programs" (Def.'s Mot. at 40). The law does not permit discovery based on defense speculation.

Exhibit 20

National Security

Justice is reviewing criminal cases that used surveillance evidence gathered under FISA

By **Sari Horwitz** November 15, 2013

The Justice Department is conducting a comprehensive review of all criminal cases in which the government has used evidence gathered through its warrantless surveillance program and will be notifying defendants in some of those cases, according to Attorney General Eric H. Holder Jr.

“We have a review underway now,” Holder said in an interview with The Washington Post. “We will be examining cases that are in a variety of stages, and we will be, where appropriate, providing defendants with information that they should have so they can make their own determinations about how they want to react to it.”

In the wide-ranging interview on Thursday, Holder also discussed the prosecution of the alleged Boston Marathon bomber, efforts to bring former NSA contractor Edward Snowden back to the United States, leak investigations and some of his plans.

“I’ve made the determination — I’m not sure I’ve ever said this publicly — but I’m going to certainly stay in this job well into 2014,” Holder said during a flight from Peoria, Ill., to Washington. “If you had asked me that six months ago, I’m not sure I would have given you that answer. I think I probably would have come up with a shorter time frame. But given the issues that I want to focus on and given the condition that they’re in, I think that staying into 2014 is necessary, but also something that I want to do.”

Holder said he will decide by mid-January whether to seek the death penalty if Dzhokhar Tsarnaev, 20, is convicted in the Boston bombing. He said he will review separate recommendations by Carmen Ortiz, the U.S. attorney in Boston; a Justice Department review committee; Deputy Attorney General James M. Cole; and Channing Phillips, counselor to the attorney general.

“I’ve asked people at every layer — to the extent that they can — to take a fresh look at it so that I’m getting a bunch of different perspectives and not a repeat of whatever the initial or the latest recommendation is,” Holder said. They will take

into account the offenses, the background and age of Tsarnaev, and his alleged role in the crimes.

“But at the end of the day, it’s going to be me with a large stack of paper . . . sitting at my kitchen table while everybody else in my house has gone to sleep,” Holder said. “And over the course of a few days, I will sit down and make the determination.

“It’s the single most weighty thing I do as attorney general,” Holder said.

Holder said that Justice officials have not given up on efforts to repatriate Snowden, who has received temporary asylum in Russia, to stand trial on charges under the Espionage Act for taking and leaking classified documents about surveillance programs. He said conversations with Russian officials “if not constant are ongoing.”

He said that “as of now,” Russian officials are not receptive to sending Snowden back for trial.

Holder indicated that the Justice Department is not planning to prosecute former Guardian reporter Glenn Greenwald, one of the journalists who received documents from Snowden and has written a series of articles based on the leaked material. Greenwald, an American citizen who lives in Brazil, has said he is reluctant to come to the United States because he fears detention and possible prosecution.

“Unless information that has not come to my attention is presented to me, what I have indicated in my testimony before Congress is that any journalist who’s engaged in true journalistic activities is not going to be prosecuted by this Justice Department,” Holder said.

“I certainly don’t agree with what Greenwald has done,” Holder said. “In some ways, he blurs the line between advocate and journalist. But on the basis of what I know now, I’m not sure there is a basis for prosecution of Greenwald.”

Greenwald said he welcomed the statement but remains cautious.

“That this question is even on people’s minds is a rather grim reflection of the Obama administration’s record on press freedoms,” he said in an e-mail. “It is a positive step that the Attorney General expressly recognizes that journalism is not and should not be a crime in the United States, but given this administration’s poor record on press freedoms, I’ll consult with my counsel on whether one can or should rely on such caveat-riddled oral assertions about the government’s intentions.”

The disclosure about the review of criminal cases comes just weeks after the Justice Department informed a suspect for the first time that it intends to use evidence against him gathered through the government’s warrantless surveillance program under the Foreign Intelligence Surveillance Act.

The Justice Department’s notifications are likely to lead to a constitutional challenge to surveillance law, which allows electronic communication between foreign targets and people in the United States to be intercepted. The Supreme Court had previously declined to hear a challenge to the law because litigants could not prove that they had been monitored.

Holder said he did not know how many cases are involved, but he said the notifications will be made on a rolling basis as Justice Department officials find the information.

The notifications could, in some instances, involve cases in which defendants have already been convicted and are in prison. In those matters, defense attorneys may try to reopen the cases.

For the first time last month, the Justice Department informed a terrorism suspect in Colorado that it intends to use “information obtained or derived from acquisition of foreign intelligence information conducted pursuant to the Foreign Intelligence Surveillance Act.”

The notification came in the case against Jamshid Muhtorov, a refugee from Uzbekistan who lives in Aurora, Colo. He was charged in 2012 with providing material aid to the Islamic Jihad Union, and he and another man were suspected of trying to participate in a terrorist attack planned by the group.

That first notification came after a vigorous internal debate last summer between lawyers in the National Security Division and Solicitor General Donald B. Verrilli Jr., who argued that there was no legal basis for withholding disclosure, according to an administration official who spoke on the condition of anonymity to discuss the sensitive matter.

The National Security Division lawyers had argued that it was not necessary to make the notifications unless the evidence derived from the wiretap or intercepted e-mail was introduced directly into the case, the official said. Eventually, Verrilli won out.

Julie Tate contributed to this report.

Sari Horwitz covers the Justice Department and criminal justice issues nationwide for The Washington Post, where she has been a reporter for 30 years. [🐦 Follow @sarihorwitz](#)

Share news tips with us confidentially

Do you have information the public should know? Here are some ways you can securely send information and documents to Post journalists.

Learn more

Exhibit 21

[Senate Hearing 113-601]
[From the U.S. Government Publishing Office]

S. Hrg. 113-601

OPEN HEARING TO CONSIDER THE NOMINATIONS
OF JOHN P. CARLIN AND FRANCIS X. TAYLOR

=====

HEARING
BEFORE THE
SELECT COMMITTEE ON INTELLIGENCE
OF THE
UNITED STATES SENATE
ONE HUNDRED THIRTEENTH CONGRESS
SECOND SESSION

TUESDAY, FEBRUARY 25, 2014

Printed for the use of the Select Committee on Intelligence

[GRAPHIC NOT AVAILABLE IN TIFF FORMAT]

Available via the World Wide Web: <http://www.fdsys.gov>

93-212 PDF

U.S. GOVERNMENT PUBLISHING OFFICE
WASHINGTON : 2015

For sale by the Superintendent of Documents, U.S. Government Publishing Office,
<http://bookstore.gpo.gov>. For more information, contact the GPO Customer Contact Center,
U.S. Government Publishing Office. Phone 202-09512091800, or 866-09512091800 (toll-free).
E-mail, gpo@custhelp.com.

SELECT COMMITTEE ON INTELLIGENCE

[Established by S. Res. 400, 94th Cong., 2d Sess.]

DIANNE FEINSTEIN, California, Chairman
SAXBY CHAMBLISS, Georgia, Vice Chairman

JOHN D. ROCKEFELLER IV, West Virginia	RICHARD BURR, North Carolina
RON WYDEN, Oregon	JAMES E. RISCH, Idaho
BARBARA A. MIKULSKI, Maryland	DANIEL COATS, Indiana
MARK UDALL, Colorado	MARCO RUBIO, Florida
MARK WARNER, Virginia	SUSAN COLLINS, Maine
MARTIN HEINRICH, New Mexico	TOM COBURN, Oklahoma
ANGUS KING, Maine	

HARRY REID, Nevada, Ex Officio
MITCH McCONNELL, Kentucky, Ex Officio
CARL LEVIN, Michigan, Ex Officio
JAMES INHOFE, Oklahoma, Ex Officio

David Grannis, Staff Director
Martha Scott Poindexter, Minority Staff Director
Desiree Thompson-Sayle, Chief Clerk
CONTENTS

FEBRUARY 25, 2014

OPENING STATEMENTS

Feinstein, Hon. Dianne, Chairman, a U.S. Senator from California.	1
Chambliss, Hon. Saxby, Vice Chairman, a U.S. Senator from Georgia	2

WITNESSES

General Francis X. Taylor, Nominee, Undersecretary for Intelligence and Analysis, Department of Homeland Security.....	4
Prepared Statement.....	7
John P. Carlin, Nominee, Assistant Attorney General for National Security, Department of Justice.....	11
Prepared Statement.....	13

SUPPLEMENTAL MATERIAL

Questionnaire for Completion by Presidential Nominees--Taylor....	32
Additional Prehearing Questions--Taylor.....	64
Letter dated February 21, 2014, from International Association of Chiefs of Police supporting General Taylor's Nomination.....	87
Questionnaire for Completion by Presidential Nominees--Carlin....	88
Additional Prehearing Questions--Carlin.....	108

OPEN HEARING TO CONSIDER THE

NOMINATIONS OF JOHN P. CARLIN

AND FRANCIS X. TAYLOR

TUESDAY, FEBRUARY 25, 2014

U.S. Senate,
Select Committee on Intelligence,
Washington, DC.

The Committee met, pursuant to notice, at 2:30 p.m., in Room SD-526, Dirksen Senate Office Building, the Honorable Dianne Feinstein (Chairman of the Committee) presiding.

Committee Members Present: Senators Feinstein, Chambliss, Wyden, Udall (of Colorado), Heinrich, King, Collins, and Coburn.

OPENING STATEMENT OF HON. DIANNE FEINSTEIN, CHAIRMAN, A U.S. SENATOR FROM CALIFORNIA

Chairman Feinstein. We meet today to consider two intelligence positions, President's nominations for those positions. One is Mr. John Carlin, a very young-looking nominee to be assistant attorney general for national security in the Department of Justice; and the other is the slightly more mature General Frank Taylor, the nominee to be undersecretary of homeland security for intelligence and analysis.

We have votes scheduled for 3:30, so my hope is we can be succinct to the point and be able to conclude this hearing within that time. But I'd like to begin by saying welcome to you both, and particularly to your family and friends who are here with you today.

The two positions for which these nominees have been nominated were both created as a part of reform efforts in the past decade after major intelligence failures, including most specifically the terrorist attacks of September 11th, 2001. The assistant attorney general for national security in the National Security Division of the Department of Justice that Mr. Carlin would lead, if confirmed, is intended to bring together the counterterrorism, intelligence, and counterintelligence efforts within the Department of Justice.

The National Security Division conducts oversight of FBI national security investigations and has the lead within DOJ for reviewing and approving requests to the FISA Court for surveillance activities. Increasingly important, the assistant attorney general must also ensure that when terrorists, proliferators, and spies against America come into our custody, our response strikes the proper balance between gathering intelligence from them and being able to prosecute them.

Mr. Carlin is well-suited to the position, having served as the acting assistant attorney general since his predecessor, Lisa Monaco, went to the White House last year to become President Obama's top adviser for counterterrorism and homeland security.

Mr. Carlin was previously the principal deputy assistant attorney and chief of staff for the National Security Division in 2011. He served in leadership positions at the FBI, including chief of staff to FBI Director Bob Mueller. He served in a variety of positions in the department between 1999 and 2007.

Our other distinguished nominee, General Frank Taylor, has a long career in national security, starting with his 31-year career in the United States Air Force, most of which was spent in the counterintelligence field. In 2001, he was named the coordinator for counterterrorism, the senior-most counterterrorism position in the State Department, and then assistant secretary of state in charge of diplomatic security.

He spent the past nine years in the private sector, during most of which time he was the chief security officer for General Electric. In that position, he has seen the government's national and homeland security functions from the outside, giving him an important perspective on the Department of Homeland Security's support to nonfederal positions, partners, and stakeholders--specifically, the private sector.

General Taylor will have to put his leadership skills and experience to good use as undersecretary of DHS for intelligence and analysis. The office, like the department as a whole, has a large number of missions to accomplish, with a long history and precedent to rely on.

I'm going to cut my remarks short and put the remainder in the record and recognize the distinguished vice chairman for his remarks.

OPENING STATEMENT OF HON. SAXBY CHAMBLISS, VICE CHAIRMAN, A
U.S. SENATOR FROM GEORGIA

Vice Chairman Chambliss. Well, thanks Madam Chair, and to Mr. Carlin and General Taylor, I join the chair in welcoming you to this Committee and congratulating you on your nomination by the President.

Mr. Carlin, since Congress created the National Security Division as part of the post-9/11 effort to tear down the walls between the criminal and national security worlds, NSD has taken on a key role in our nation's intelligence collection activities. In the wake of the Snowden leaks, I understand the administration may be making some changes, especially to section 702 of FISA that will negatively impact how our intelligence agencies collect and retain information.

When Congress passed the FISA Amendments Act, we were careful to not put up walls or prohibit lawfully collected information from being used. I hope you'll be a strong voice against any policies that try to undo the intent behind the FAA and that make it harder for our intelligence agencies to do their jobs.

When you and I met in my office, we had a good discussion about this administration's ongoing failure to come up with an interrogation and detention policy that would allow for the collection of real-time, actionable intelligence, without defense attorneys, Miranda rights, or judicial deadlines.

As a prosecutor, you understand there is no requirement to give a terror suspect Miranda rights. It just means you can't use his statements at trial. Captured terrorists can be gold mines for information that we should need, and therefore we should not treat them like ordinary criminals.

Unless we can get good intelligence from these detainees, we could fall behind the curve in preventing future attacks. That's the risk that should not be acceptable to anyone, regardless of any campaign promise.

NSD is also at the forefront of terrorism and counterintelligence investigations throughout the country. While the criminal justice system clearly plays an important role in national security thesis, I believe we should do more to make our military commission system a success. Now is not the time to bring dangerous criminals, dangerous terrorists, into the United States and give them the benefits of our criminal justice system. There is simply too much uncertainty following an acquittal, as we recently saw with the unsuccessful prosecution of the Somali pirate in federal court, here in the district.

General Taylor, we thank you for returning to government to take on this new assignment: one that promises to be as difficult as any in your career, as you and I discussed a little earlier. Census creation, nearly a decade ago, DHS I&A, has struggled to find an organizational identity to fit in with

the Intelligence Community and to attain the level of professional competence that the American people are entitled to expect in their government.

For some time now, Members of Congress, on both the House and the Senate, and on both sides of the aisle, have questioned the very existence of I&A and the work that it does. Their questions about the quality and necessity of much of INA's analysis, concerns about INA's ability to process and share information, questions about the size of the workforce in relationship to its level of production, and concerns about the potential for DHS to safeguard cyber and critical infrastructure. All of these questions come at a time when I&A is still clinging to a corporate notion that it is a new organization.

My comments are not intended to disparage the professional men and women who work for DHS. There are an awful lot of very capable, very professional individuals involved there, many of whom have begun to ask these same questions. Rather, my concern lies with the inability of I&A as a whole to routinely demonstrate a unique contribution to the national security of the United States.

General, if confirmed, you may be the last, best hope for the future of DHS I&A. It's unlikely you will be able to keep I&A aloft by maintaining the current course in hitting, so I would like your candid thoughts about what you plan to do over the next 12 months to fix I&A for the long term.

I have great confidence in Secretary Johnson. Secretary Johnson has great confidence in you. Therefore, I transfer that confidence, myself, to you. I look forward to our discussion today, and working with both of you in the future, and I thank you Madam Chair.

Chairman Feinstein. Thank you very much, Mr. Vice Chairman. Gentlemen, would you stand and I'll administer the oath?

[Witnesses comply.]

Chairman Feinstein. Please affirm when I finish reading.

Do you solemnly swear that you will give this Committee the truth, the full truth, and nothing but the truth, so help you God?

[Witnesses respond affirmatively.]

Chairman Feinstein. Thank you, you may be seated.

And just a couple of questions--this is pro forma. Please answer yes or no.

Do you both agree to appear before the Committee here or in other venues when invited?

[Witnesses respond affirmatively.]

Chairman Feinstein. Do you both agree to send officials from your respective offices to appear before the Committee and designated staff when requested?

[Witnesses respond affirmatively.]

Chairman Feinstein. Do you both agree to provide documents or any other materials requested by the Committee in order for it to carry out its oversight and legislative responsibilities?

[Witnesses respond affirmatively.]

Chairman Feinstein. Will you both ensure that your respected offices and its staff provide such material to the Committee when requested?

[Witnesses respond affirmatively.]

Chairman Feinstein. Do you both agree to inform and fully brief to the fullest extent possible all Members of this Committee, of intelligence activities and covert actions, rather than only the chairman and vice chairman?

[Witnesses respond affirmatively.]

Chairman Feinstein. Thank you very much. And if you would proceed and make your statements, and introduce your family or whomever you'd like to introduce in general, I'll go to seniority and ask you to speak first.

STATEMENT OF GENERAL FRANCIS X. TAYLOR, NOMINEE FOR
UNDERSECRETARY OF HOMELAND SECURITY FOR INTELLIGENCE AND
ANALYSIS

General Taylor. I'm honored and extraordinarily humbled to appear before you today as the President's nominee for the undersecretary for intelligence analysis at the Department of Homeland Security. With me today is my elder son Jacquis, sitting behind me, representing our family. My wife is now in London visiting our daughter, who is studying to be a solicitor, and could not join us--she had already had this trip planned. So she's with us in spirit. I talked to her this morning.

During my last period of government service, I was privileged to have the opportunity to work with Governor Ridge and his team as they endeavored to establish this new department in 2003. The department has come a long way since those early days, especially I&A, as its mission and responsibilities have continued to evolve.

This position, and the team that I would be privileged to lead if confirmed, is a crucial link between the federal government and the Intelligence Community, with our state, local, tribal, and territorial partners, as well as the private sector that are on the front lines every day to protect our country and our citizens from an ever-evolving threat.

As we learned in the aftermath of 9/11, security of this nation requires effective collaboration at every level of our country. Sharing information, both from the federal government as well as from our local partners to the federal government provides clear understanding of the nature of the threats that we face, and allow all levels to be on the same sheet of music. I remain haunted by the fact that at least one of the 9/11 hijackers were engaged by local law enforcement before the attack, and their potential action against that person could not be accomplished.

That is why we strive to create--that I will strive to create, if confirmed, I will work to strengthen and improve the process of how this partnership works to identify and act on potential threats to our country and our citizens. If confirmed, I believe my 43 years of law enforcement, security intelligence, and crisis management experience provides the right skills to build on the significant work of my talented and dedicated predecessors.

I've had the distinct honor to serve our country as a leader of two global investigative and security organizations, as a U.S. ambassador directing diplomatic counterterrorism efforts, and diplomatic security operations. I also had the privilege of serving as the chief security officer for a Fortune 10 global U.S. conglomerate, the General Electric Company. In each of these roles, I have been responsible for mission execution and mission success, and I believe my record indicates consistent successful results in these very different roles. I've had both line and staff roles, worked in policy, developed, and executed budgets at every level, and led operational activity to mitigate risk to our country both in the U.S. and abroad and, as well, to an American economic giant.

I understand that the I&A mission is different from any of the--of my past responsibilities, and that I will have to endeavor to learn the organization, its customer requirements, its successes, and its opportunities for improvement. The good news is that my initial assessment after a week of briefings is very positive about where the organization is in its development, and that there will be a firm foundation upon which for me to build.

I think there are three areas where we must focus. First, enabling the fusion centers to reach their potential with

effective information sharing and from this--to and from this important institution. Sustaining DHS's contribution to the Intelligence Community with information analysis derived from state, local, and tribal partners, and from a unique D.H. information sources. And finally, to aggressively eliminate duplicative analysis that can more effectively be done by other federal organizations.

In my view, what makes I&A unique in the Intelligence Community is its mission to link the U.S. Intelligence Community with first responders in our country. State and locally owned and operated fusion centers are critical to bringing the 18,000 police entities across our great country into the national counterterrorism fight. Caryn Wagner, as well as the current I&A leadership team, began that process with the aggressive deployment of I&A personnel to the fusion centers and the development of a program of analysis that will guide the future production of our analytical products.

If confirmed, I will work relentlessly on executing these plans to ensure all understand the critical aspect of the I&A mission is the nature and effectiveness of how we support our state, local, tribal, and public sector partners. Finally, I am acutely aware that no organization can live on its reputation or hide behind its mission statement. Organizations must continue to evolve and improve to meet changing environment that they must operate in. Mission assessment, the development of clear objectives, and rigorous metrics will help I&A stay focused on the present and the future. In my initial briefings, again, I am impressed by what I have seen as a baseline to set expectations and measure effectiveness.

If confirmed, I plan to sustain these efforts and use these results as a basis for adjustments to the organization and mission execution. Madam Chairman, I'd like to submit the rest of my statement for the record and would conclude with those thoughts.

[The prepared statement of General Taylor follows:]

[GRAPHICS NOT AVAILABLE IN TIFF FORMAT]

Chairman Feinstein. Excellent. Thank you, General Taylor. Mr. Carlin.

STATEMENT OF JOHN P. CARLIN, NOMINEE FOR ASSISTANT ATTORNEY GENERAL FOR NATIONAL SECURITY IN THE DEPARTMENT OF JUSTICE

Mr. Carlin. Thank you, Madam Chairman and Vice Chairman Chambliss, and distinguished Members of this Committee. It's an honor to appear before you today, and I thank you for considering my nomination. I'd like to thank the President for his confidence in nominating me, and the Attorney General for his support.

Chairman Feinstein. Could you please introduce your family to us, because, there's one little girl that's through (ph) with expectation.

[Laughter.]

Mr. Carlin. She is. Thank you. I'd like to introduce them, and thank them for their love and support over the years--a few years, in one case: My wife Sarah and our daughter Sylvie; my parents, Roy and Patricia, who traveled here from New York City; and my mother in-law, Jura Newman.

I also want to thank my wife for her countless sacrifices to allow me to pursue a career in public service; and to thank my parents who always taught my sister and me, both by lesson and by example, the importance of dedication, discipline and always doing what's right.

With the support of all of my family and their selflessness, I've been able to choose the path that's led me here today. And I'd like to thank the people from the National

Security Division in the department who've come here, along with friends, to show their support today.

It's been a true privilege to spend my entire legal career with the Department of Justice and to witness a time of enormous transformation after the terrible events of September 11th. As with so many Americans, I and my family recall vividly the events of that day--the horror of senseless murder and the dark cloud of ash that hovered over New York City.

My brother-in-law was across the street from the twin towers and my father was in the subway underneath. And I remember as our family called each other to determine that we were safe. We were lucky.

Our core mission at the National Security Division is clear: to prevent future terrorist attacks, while preserving our civil liberties. And it's a special honor and privilege to be considered for a position charged with leading the division that Congress, and this Committee in particular, created to unite all the Department of Justice's national security elements to bring all tools to bear in the fight against terrorism and other threats to national security.

Serving as the acting assistant attorney general for national security for approximately the last 11 months, I've been both humbled and driven by the responsibilities and mission entrusted to this position. For more than a decade, I've learned from and worked alongside some legendary public servants as the United States undertook fundamental changes in our approach to combating the threat of terrorism and other emerging national security challenges.

In particular, working with FBI Director Bob Mueller as a special counsel, and later as his chief of staff, to help the bureau evolve from a law enforcement agency into a threat-based intelligence-driven national security organization. Here at NSD, we must apply and are applying those lessons, both to meet the growing national security cyber-threat and to continue to evolve to meet other changing national security threats.

If I am fortunate enough to be confirmed, I look forward both to continuing this important evolution and to working with this Committee in its essential oversight role.

Thank you again for the opportunity to appear before you today, and for your consideration, and I look forward to answering your questions.

[The prepared statement of Mr. Carlin follows:]
[GRAPHICS NOT AVAILABLE IN TIFF FORMAT]

Chairman Feinstein. Thank you both very much.

We will proceed in our usual order, which is early bird regardless of party.

Mr. Carlin, in your answers to the Committee's pre-hearing questions, you wrote the DOJ's National Security Division, quote, ``oversees all electronic surveillance and other activities conducted under the Foreign Intelligence Surveillance Act.'' So I know you have direct experience with DOJ oversight provided to FISA activities. Based on that experience, I'd like you to run through and explain, so the public understands, the various layers of oversight that the programs authorized by FISA, such as sections 215 and 702 data collection programs are subject to.

Mr. Carlin. Thank you, Madam Chairman.

And there are different layers. I'll try to walk through the different functions that are performed.

First, at the agency that performs the collection activity, there will be supervisory oversight and Office of Compliance. Next, there will be the general counsel of that agency who will be informed of what the rules are, depending on the applicable authority, and be responsible for teaching and enforcing those rules.

Then there will be the inspector general for the particular

agency involved. There will also be the inspector general for the Intelligence Community writ large, and the Office of the General Counsel for the director of national intelligence.

The National Security Division plays an oversight role as well, conducting review of the use of the authority and, depending on the particular incidents of the use of the authority, overseeing the application to another oversight element, which is that of the Foreign Intelligence Surveillance Court.

Those are judges--just the same judges I appeared before literally in some cases when I appeared in criminal court, that have been tapped to appear in their Article III role, in addition to their normal duties as part of the Foreign Intelligence Surveillance Court.

And finally, there is this Committee in particular, and the intelligence committees in Congress who have a particular oversight role in these areas and are kept current--currently and fully informed of the activities under the FISA Act.

Chairman Feinstein. OK. It's my understanding that NSD does not generally conduct oversight of CIA human intelligence activities; covert action; three, DOD military activities; or four, NSA intelligence collection outside of FISA. As I understand it, within the Department of Justice, only the Office of Legal Counsel weighs in on these matters and then even only when they're asked.

So here's the question. Should NSD play a role in reviewing the legality of intelligence collection outside of FISA by CIA, NSA and others?

Mr. Carlin. Thank you. I--the division does not have the, as you have stated, Madam Chairman, a formal oversight role for other particular authorities. But we were created to serve as a bridge between the Intelligence Community on the one hand, and the Department of Justice and the law enforcement elements on the other, to ensure that the wall came down in terms of sharing of information and that there was visibility into the activities of the Intelligence Community.

There are areas where we have a particular expertise, such as FISA. We're also assigned a role in terms of the attorney general's approval of attorney general guidelines that would get issued by the relevant agency, but then to the Department of Justice for approval. And there, our role would be in particular protecting the rights and privacies of U.S. persons.

So, I'd be happy to work with this Committee on areas where our expertise fits in, as we've discussed, to the general layers of oversight that otherwise exist within the Community, including inspectors general and general counsels.

Chairman Feinstein. Thank you. We will take you up on that.
Mr. Vice Chairman.

Vice Chairman Chambliss. Thanks, Madam Chair.

General Taylor, you have said that one of your top priorities is to enhance the level of service that I&A provides to its unique customers in the private sector and at state and local levels. I&A has had historically low analytic production. For example, in 2012, it produced fewer analytic products than its total number of employees. How do you plan to increase the number of high-quality analytic products that are available for INA's customers without being redundant with other Intelligence Community efforts?

General Taylor. Senator, thank you for that question. I think it's not simple, but it's kind of focusing on what's the mission of I&A. And the mission of I&A is to collect information from our state and local partners and turn that into intelligence that can be used in the Intelligence Community; to work specifically with the Intelligence Community to get information back to our state and local and private sector partners.

But I think also to use the unique information within the

department to produce intelligence. That is where we're going to focus. It's my view that that's not all happening as much today as it needs to happen going forward. But I intend to focus on those products that meet those kinds of needs.

I would also add that the analytical products that I think the Committee has seen in the past are not the only products that we get asked--that I&A is asked to deliver. So one of the metrics that I'm thinking of looking at is what is the totality of the product base that I&A delivers? Where does it go? What are the customers saying about it? And then coming back to the Committee with a better understanding, or better picture of the totality of the work done by I&A, except--rather than just analytical products.

Vice Chairman Chambliss. As we all know, CIA has jurisdiction of intelligence collection outside the United States. FBI has jurisdiction of intelligence collection within the United States' borders. The relationship between I&A and the FBI has not been what it really should be. I understand you're a friend of Director Comey, who is starting off certainly in the right direction at the FBI. He's had vast experience at the Department of Justice.

Can you talk about how you expect to develop that relationship between I&A and the FBI to make sure that we're doing the best job we can within the borders of the United States to not only collect intelligence, but also provide the right analysis of that intelligence?

General Taylor. Yes, sir. I--in my 43 years of government service have worked closely with the FBI at every level. I would tell you that I am not a person that believes in competitive--working to compete against an agency. I believe in building partnerships that look to the strength of each agency in performing the mission.

So I commit to you that I will work with Director Comey and his team to make sure that what I&A is doing is complementing what he's doing, and we're complementing what the FBI is doing in a synergistic fashion. There's just far too much for us to do to be competing with each other. We should be able to work collectively for the best interests of our country and for collecting intelligence that defends America.

Vice Chairman Chambliss. Mr. Carlin, a number of groups and organizations have been making recommendations on how to fix FISA in response to Edward Snowden's leaks of classified information. Some of these recommendations have been good, but a lot of them seem to be unworkable, both from a legal as well as a practical standpoint, and would in fact damage our national security collection efforts.

Number one, do you believe NSA's telephone bulk metadata collection program fully complies with U.S. law?

Mr. Carlin. I do.

Vice Chairman Chambliss. Three of the five members of the privacy and civil liberties oversight board have said that the plain text of FISA business records statute does not authorize this bulk collection--bulk meta data collection program.

What aspects of their legal analysis do you find to be problematic?

Mr. Carlin. Just say--Senator that--do believe that it is the correct interpretation of the statute and that it is Constitutional as have 15 FISA court judges and now two district court judges. There is one judge who has found to the contrary. We have taken that case--the Department has taken that case up on appeal and it's being litigated in the court system.

Senator King. Well, all right I'll leave your answer at that then. Very loose answer though, Jim (ph).

Let me just lastly--quickly ask you, in your experience with the Foreign Intelligence Surveillance Court do you think it's been anywhere--anything like a rubber stamp?

Mr. Carlin. I--no sir. I have not. It's--as I've said, today--but these are some of the same district court judges that I appear before in the criminal court. And they are respected jurists. They put us to our paces when I was a government lawyer appearing before them then. And they put us to our paces when they perform the same role in front of the Foreign Intelligence Surveillance Court.

And I think some of the opinions in this unprecedented year of de-classifying thousands of pages of documents, I think some of the court opinions have shown the type of rigor that they've applied to their analysis.

Senator King. OK, thank you.

Chairman Feinstein. Thank you very much, Mr. Vice Chairman. Senator Wyden.

Senator Wyden. Thank you, Madam Chair.

Mr. Carlin I enjoyed very much visiting with you and as I indicated, if you're confirmed, you're gonna be responsible for overseeing a range of government surveillance activities and to be blunt, you're gonna have a lot of cleaning up to do.

For years, the Justice Department has allowed the executive branch to rely on a secret body of surveillance law that was inconsistent with the plain meaning of public statutes in the Constitution. This reliance on secret law gave rise to a pervasive culture of information in which senior officials repeatedly made misleading statements to the Congress, the public and the courts about domestic surveillance.

For example, officials from the National Security Division testified on multiple occasions that Section 215 of the PATRIOT Act was analogous to grand jury subpoena authority, which of course involves individual suspicion.

The public can now see that this claim was extraordinarily misleading and the National Security Division's credibility has been damaged as a result.

If you're confirmed to head the National Security Division, what are you going to do to end this culture of misinformation and ensure that statements made to the public, the Congress and the courts by the Department are accurate?

Mr. Carlin. Thank you, Senator.

I think it is of the utmost importance--and the attorneys I've worked with at the National Security Divisions share this view--that when we testify, whether it's before Congress or provide information to the courts or in other settings that we do our utmost to provide the full and complete and accurate information.

If I may on the issue that arises in terms of 215 and grand jury subpoenas, it is of course in the statute itself the provision that the records that one can obtain through 215 need to be those records--similar to those records that one could obtain by a grand jury subpoena as it says in the statute or other court process.

Two-fifteen is different than the issuance of a grand jury subpoena in part because of--one needs to apply to a judge prior to being able to obtain the authority. And I know that lawyers at the National Security Division and the department and elsewhere work to make sure that those portions at the time that were classified in terms of the applications of 215 were provided not just to this Committee as would be the normal course of business, but to ensure that, that interpretation of the law was made available to all Members of the Senate prior to the consideration of the 215.

I--inclusion again, I believe it's very important to try to provide as accurate information, as complete information as possible to this Committee and to this body whether in classified or unclassified...

Senator Wyden. If you're confirmed, I hope that will be accurate in the future, because I know when people heard those words, that this was analogous to a grand jury subpoena

process, they said those kinds of processes involve individual suspicion. And, frankly, I don't know of any other grand jury subpoena that allow the government to collect records on this kind of scale.

So I'm gonna move on.

You've indicated that you are going to make a priority insuring that statements that are made, if you're confirmed, are accurate. In my view, that was not the case in the past.

Let me ask you one other question, if I might.

As the arguments in favor of bulk phone records collection have been crumbling, executive branch officials most recently have claimed that bulk collection allows the government to review phone records more quickly than would otherwise be possible.

One official recently testified that it allows the government to do in minutes what would otherwise take hours. However, the Justice Department inspector general's January 2010 report, on requests for phone records, describes an arrangement in which communications companies were able to respond to requests immediately and provide records in a format that could be immediately uploaded onto FBI databases.

While the inspector general found some problems with the--with this particular arrangement, speed was not one of them. In fact, the report goes on to note that the FBI's counterterrorism division described this arrangement as providing near real time servicing of phone record requests.

Would it be fair to say that this report--a Justice Department report--indicates that phone companies are actually capable of responding to individual record requests very quickly?

Mr. Carlin. Senator, I'm not totally familiar with the details of that inspector general report or whether that arrangement still exists at the FBI.

But it has certainly been my experience, in the context of some particular cases--investigations that I can recall with a particular telecommunications companies that we have served particular requests on the company and that they have been able to respond very, very quickly to the FBI. And that, that speed has been critical in having that national security investigations hold people to account or to prevent future terrorist attacks, and that speed is critical.

Senator Wyden. Well I share your view that speed is critical, but what we have is a FBI in effect Justice Department inspector general report indicating that it's possible to get that speed that we need with the kind of approach with respect to phone records without collecting other kinds of--without other kinds of processes, and that's my point, is that we're told that without metadata collection, we're not going to get it in a timely way. This report indicates that it is possible to get it in a timely way.

Thank you, Madam Chair.

Chairman Feinstein. Thank you very much.

[Cross talk.]

Senator Udall. Thank you, Madam Chair.

Good afternoon, General Taylor.

Good afternoon, Mr. Carlin.

Mr. Carlin, let me turn to you for a series of questions. Last May, the White House formally announced that if a lethal operation will be considered against a U.S. person, that the Department of Justice--and I want to quote here--`will conduct an additional legal analysis to ensure that such action may be conducted against the individual, consistent with the Constitution and laws of the United States.'

Two questions: What's the role of the NSD in that kind of a review? And who in the DOJ is responsible for ensuring that the facts supporting the department's legal analysis are accurate?

Mr. Carlin. Thank you, Senator.

In--there's a process set up that involves input from each of the departments and agencies now, before such a decision of that magnitude is made. That's the policy process that's been set up by the President.

In terms of the extra legal analysis might occur, a decision of that magnitude would be made at the highest level of the department. And I would expect that before such a decision would be made, that the National Security Division, among other components, would be consulted.

On the second question, in terms of the accuracy of the information that's provided, the accuracy of the information is usually determined by the departments and agencies providing it. So there's the collectors and the analysts. And they would provide, then, that information to the department and that would be the basis for a legal review.

Senator Udall. Over time, I'm going to want to drill more into those questions. Because this is, as you know, a life-and-death kind of process. But let me--let me turn to another question that's about accuracy.

You wrote in your responses to the Committee that the decision to submit intelligence activities for legal review by the OLC is typically made by the Intelligence Community component that engages in that activity. Yet you also wrote that the NSD has the responsibility to ensure that the department's representations in court are accurate, and that, quote, ``the NSD attorneys must work diligently to understand the facts of intelligence activities and other national security- related matters that may be at issue in litigation or other matters for which they're responsible.''

Now, to me, those statements appear to conflict with each other. So in your view, how is the Justice Department supposed to ensure the accuracy of representations to the courts in criminal cases or FOIA litigation, I should say, and so on, without an independent review of the accuracy of Intelligence Community representations?

And I ask that question in light of what former CIA General Counsel Stephen Preston's responses to my questions last year about the CIA's detention and interrogation program, where--and he wrote that the DOJ does not always have accurate information about the detention and interrogation program and that the actual conduct of that program was not always consistent with the way the program had been described to the DOJ, and that further, CIA's efforts fell well short of our current practices when it comes to providing information relevant to the OLC's legal analysis.

Mr. Carlin. Thank you, Senator.

Your question is important and it's important as officers of the court. And any attorney for the National Security Division when making a representation does everything that they can to assure that the representation is accurate.

And also if they were to learn or discover that information is inaccurate or misleading, to take steps with the relevant agency in order to correct the record.

There were several different decision-making processes that you've alluded to, some of which are more involved with than others. So in terms of representations before the Foreign Intelligence Surveillance Court, that is one where our attorneys would be working to make the representations; would be working with the relevant elements of the Intelligence Community in order to provide the necessary facts to the court.

And as I described earlier to the chairman, there are a variety of mechanisms, including the attorneys, to try to ensure that accuracy, including the Office of General Counsel, the component of various inspectors general, and our oversight role and section.

Senator Udall. I'm going to stay involved with you on this, as I am with the Intelligence Community itself. Let me--one

last question. I want to talk about executive order 12333, with which you're familiar. I understand that the collection, retention or dissemination of information about U.S. persons is prohibited under executive order 12333, except under certain procedures approved by the attorney general. But this doesn't mean that U.S.-person information isn't mistakenly collected, retained and then disseminated outside of these procedures.

So take this example. Let's say the NSA is conducting what it believes to be foreign collection under E.O. 12333, but discovers in the course of this collection that it also incidentally collected a vast trove of U.S.-person information. That U.S.-person collection should not have FISA protections. What role does the NSD have in overseeing any collection, retention or dissemination of U.S.-person information that might occur under that executive order?

Mr. Carlin. Senator, so generally, the intelligence activities that NSA would conduct pursuant to its authorities under 12333 would be done pursuant to a series of guidelines that were approved by the attorney general, and then ultimately implemented through additional policies and procedures by NSA.

But the collection activities that occur pursuant to 12333, if there was incidental collection, would be handled through a different set of oversight mechanisms than the department's by the Office of Compliance, the inspector general there, the general counsel there, and the inspector general and general counsel's office for the Intelligence Community writ large, as well as reporting to these committees as appropriate.

Senator Udall. So you don't see a direct role for the NSD in ensuring that that data is protected under FISA?

Mr. Carlin. Under FISA, no. Under FISA, we would have a direct role. So if it was under--if it was collection that was pursuant to the FISA statutes, so collection targeted at U.S. persons, for example, or collection targeted at certain non-U.S. persons overseas that was collected domestically, such as pursuant to the 702 collection program, that would fall within the scope of the National Security Division.

That's information that--and oversight that we conduct through our oversight section, in conjunction with the agencies. And we would have the responsibility in terms of informing--working with them to inform the court if there were any compliance incidents and making sure that those compliance incidents were addressed.

Senator Udall. Thank you. My time is obviously expired. But I think you understand where I'm coming from here. One is to make sure that DOJ and you in your capacity have the most accurate information so that you can represent the United States of America and our citizens in the best possible way. And secondly, that you have a role to play in providing additional oversight. Those are all tied to having information that's factual, based on what happened.

And again, I'm going to continue to look for every way possible to make sure that that's what does happen, whether it's under the auspices of the IC or the DOJ. You all have a joint responsibility to protect the Bill of Rights.

Thank you.

[Cross talk.]

Senator Collins. Thank you, Madam Chairman.

General Taylor, I spent many years as either the chair or the ranking member of the Homeland Security Committee. And my greatest disappointment in the last Congress is that we did not enact a cyber security bill since I believe we're extremely vulnerable to attacks. And indeed, we know that every day, nation-states like China, Russia, Iran are probing our computers, leaving behind malware. Transnational criminal gangs also are invading our--our computer systems, and terrorist groups also have that as a goal.

I know that you served as chief security officer at General

Electric. I'm interested in what you believe I&A, which has the special responsibility to share information with the private sector, to be the recipient of information from the private sector, and disseminate that to governments at all levels.

What particular improvements would you like to see when it comes to information sharing?

General Taylor. Thank you, Senator Collins.

I would say that in my eight-and-a-half years at GE, I was not always happy with the quality and the consistency of information I received on threats that would impact our company writ large, and particularly cyber issues. I think that has begun to improve.

And my focus will be on ensuring that--I think I--well, two things. I think the department plays a critical role from NPPD in reaching out to the private sector. And indeed, many companies have now joined in partnership with DHS around the NPPD and critical infrastructure protection and exchanging information on a continuous basis. I think that has to continue.

But I think we've got to do a better job on the I&A side of developing the intelligence that helps companies--and not--companies the size of GE have the resources to kind of look into these things more thoroughly than many, many other American companies. Those are the companies that need to understand what the risk is; understand how they're being had. And I think we can give them that through analysis from I&A, both from the IC and from our components within DOD--within DHS.

Senator Collins. Well, I hope we'll see more analytical reports, as the ranking member pointed out. There's something really wrong when there are more employees and contractors than there are--there are analytical reports being issued.

I am very impressed with what is going on at the NCIC and I hope that you'll invite Members of this Committee, as well as the Homeland Security Committee, to come out and let them see the real-time monitoring that's done of government computers because that's an important vulnerability as well.

But the fact that we still are not sharing critical threat information, particularly with the owners and operators of critical infrastructure, is just unacceptable in this day and age. And I hope that should you be confirmed, that you will make that a priority.

General Taylor. Senator, if confirmed, that will be a top priority for me. I lived that for eight-and-a-half years and want to see what I can do to help us close that gap.

Senator Collins. Mr. Carlin, according to news reports, the charges against Ali Mohamed Ali for his alleged role in a 2008 pirate attack near Yemen have been dropped after he was partially acquitted by a jury last year. This raises the whole dispute once again of how foreigners who are brought to this country or arrested here should be handled, and whether it should be in military tribunals or in regular criminal courts.

We now have the bizarre situation where the failure to successfully prosecute a suspected terrorist, pirate in federal court has now resulted in his seeking asylum so that he can stay in this country. What's your reaction to this case? And what does it say as far as our ability to ensure that those who pose a threat to this country--foreigners who pose a threat to this country should be handled--prosecuted in federal courts versus military tribunals?

Mr. Carlin. Well, Senator, without commenting on a particular individual's application, that as you say that was a piracy case. After the increased incidence of piracy in 2011, there were a number of prosecutions of pirates. I think we did obtain convictions in 25 or 26 of those cases, and that piracy, not just due to that effort, but other international efforts, has decreased in that region, but continues to be a threat.

In general, we need to use an all-tools approach where the Article III option is one of the tools in the toolkit, but that we look at all tools whenever we face a particular case. And we look first to obtain the maximum amount of intelligence, speaking now not so much about piracy, though it's true there, particular in terrorist acts or terrorist cases, and to look to gain--obtain intelligence first, to try to prevent terrorist attacks. That needs to be our first priority.

And we also need to look to deter and disable the threat that a particular individual or group may pose. And if confirmed, I will advocate and attempt to provide as many options as possible when we're trying to make those decisions.

Senator Collins. Thank you.

[Cross talk.]

Senator Coburn. Thank you, Madam Chairman.

General Taylor, first of all, most people don't know you didn't have to do this. And the fact that you're coming back to serve again is highly admirable, and I want to thank you for that.

You said you'd read the report that Senator Levin and I put out on fusion centers. And I have to agree with a lot of what Senator Chambliss had to say.

My assessment when I talked to the people receiving the analysis from I&A and homeland security is it's not on time, it's not late, and it's not accurate. And half the time, it's old information that was collected not through the Intelligence Community, but is published data. And so the quality of the work in many instances actually is very, very poor. And so, when you--when you go and talk to people who receive them, they don't even read them. Because they think they have no value. There's no incremental increase in the value of what is being put out.

So, given that, as you look at this and see whether or not there's a capability there that we really need, I don't disagree with you about sharing threats downward. I have yet to see much information come from any fusion center into I&A, and that then comes that is both timely and accurate and not repetitive. So, I guess my question is, is if it is seen by you, after looking at this, that it's redundant and irrelevant, would you agree that maybe it ought to be minimized to where it's mainly a conduit down, and when we do get some information that needs to be forward, we can do that, rather than duplicate what's already going on?

General Taylor. Senator, first of all, thank you for your comments about my service. You may know that I began my career at Tinker (ph) Air Force Base in Oklahoma, some 43 years ago, and that was a--quite a launch place to get me here. So, I'm excited to be here to be able to serve again.

I read the report. I have heard from our stakeholders, both at the state and local level, and within the IC, and within the department. What I would commit, sir, is to a thorough analysis of what the mission is. Because I think there's some confusion in terms of the elements of I&A, in terms of what the actual mission is with regard to the fusion centers. I think it is our core responsibility. No one else in the government has this responsibility to link the locals to the IC. So, I'd like to evaluate that, develop the metrics around what we're supposed to be producing, and then, if we are able to produce those things, come back to the--to you, sir, and to the SSCI and present those results.

I think there is value, here, but I haven't had enough time to really get my arms around it, but I--if confirmed, I would expect, in very short order, to be able to do that and come back with a plan of action to implement the mission we've been assigned. And if it's not there, to not do it. And to come with that recommendation based on the facts that we find in--in a mission analysis.

Senator Coburn. Well, I appreciate, and I have a lot of confidence that you're the right man for this job at this time, and my hope is that we get some clarity as to what can be done and effectively done. One of the things that's happening, we're seeing some improvement in homeland security in a lot of areas, and like Senator Collins, we need a cyber-security bill. We know that. I think the President did a good job in terms of his executive order, but we still have a ways to go there, and it's important that the intelligence and analysis that's carried out has value, because--and the problem maybe, right now, it may be improving in value, but nobody's paying any attention to it because it hadn't had any value in the past.

So, my hope is, is that you'll have Godspeed in making that assessment and truly using metrics, your customers, of whether or not it has value.

General Taylor. Senator, you have just outlined my leadership philosophy, and that's how I've approached every mission I've been given, and I also believe it's important that as we take this journey, that we're in lockstep with this Committee in terms of what the expectations are, so I intend to spend a significant amount of time with the staff and with the Members to get feedback on what we're doing. I believe in full transparency. I believe in metrics, and if the facts take us in a way that we don't like, the facts are the facts, and we'll have to make decisions from this.

Senator Coburn. Thank you. I yield back.

Chairman Feinstein. Thanks, Senator Coburn.

Senator Heinrich.

Senator Heinrich. Thank you Madam Chairman. Mr. Carlin, General Taylor, welcome to you both. Mr. Carlin, you and I had the opportunity to talk a little bit last December, and I just wanted to follow up on one of the issues that we talked about when you came to my office.

As you know, in October of 2013, after months and months of discussion and debate in which you and the NSD were involved, DOJ adopted a new policy by which federal prosecutors would inform defendants when they were intended to--when they intended to offer evidence informed, obtained, or derived from intelligence collected under 702 of FISA. And when you and I met in December, you informed me that that policy had not yet been reduced to a formal written policy, and so, Mr. Carlin, I wanted to ask: is that process done yet, and has that policy been finalized, and if so, has it been disseminated in--in a written form?

Mr. Carlin. Thank you Senator, and thank you for having taken the time to meet prior to this hearing. Just in terms of the question. I--it is my understanding that it was the practice of the policy of the department to inform a defendant in a criminal case and give notice if there was 702 information that was going to be used against them prior to--prior to this change in practice.

The change in practice had to do with a particular set of circumstances when there was an instance where information obtained from one prong of the FISA statute 702 was used and led to information that led to another prong of FISA, Title I FISA, being used, and that when the notice was given to the defendant, that notice was referring to one type of FISA but not both types of FISA, and that is the practice that we reviewed and changed, so that now, defendants are receiving notice in those instances of both types of FISA.

The review of cases affected like that--affected by that, continues, but we have filed such notice, now, I believe in three criminal matters, including the case of Muhamad Muhamad (ph), the individual convicted by a jury of attempting to use an explosive device on the Christmas tree lighting ceremony. In reference to that case, we have now filed--there's a filing in that case that we should provide to your staff while we lay out

what our practice is, and I will ensure--I will ensure that filing is distributed to U.S. attorneys' offices across the country so they know exactly what our position is on that issue.

Senator Heinrich. That's helpful. And so you'll share with--that with the Committee as well?

Mr. Carlin. Yes sir.

Senator Heinrich. Great. Let's move on then to declassification real quick. I have a quick question on that front. And, in your response to Committee questions, you indicated that you and others within NSD meet regularly with ODNI personnel on multiple issues, and among those that you listed were classification - sorry, declassification and transparency matters. On December 29th of 2009, the President signed Executive Order 13526, which directs, among other things, that in no case shall information be classified, continue to be maintained as classified, or fail to be declassified in order to conceal violations of law, inefficiency, or administrative error, prevent embarrassment to a person, organization, or agencies, or prevent or delay the release of information that does not require protection in the interest of national security. What's NSD's role and responsibility in determining whether something is properly declassified--sorry, properly classified, particularly as it relates to that Executive Order 13526?

Mr. Carlin. Thank you Senator. NSD really does not play a role in that executive order in determining whether the information is properly classified in the first instance. That would be a decision that's made by the relevant agency or department would have expertise with the particular sources and methods and would be reviewed. Assume, ultimately, if there was a dispute by their general council or inspector general, we have played and do play a role in the ongoing review in terms of coordinating the declassification, particularly of FISA related pleadings or court opinions, and we've been playing an ongoing role in that review that has led to the declassification by the director of national intelligence and thousands of pages of documents, and I would expect we would continue to play a role in that if confirmed.

Senator Heinrich. That's very helpful, Mr. Carlin, and I want to thank you both for being here today. Thank you Chairman.

Chairman Feinstein. Thank you, Senator Heinrich

Senator King. Our wrap-up questioner.

Senator King. Thank you, Madam Chairman.

Mr. Carlin, the President made a speech on January 17th on national security policy. He called for the creation of panels of advocates to assist the FISA court. This Committee passed an amendment as part of our bill that created an opportunity for the court to appoint amicus assistants in that process. Do you have any insight on what the President had in mind in that statement, and was what we did along the lines of what the President intends?

Mr. Carlin. Not sure, Senator, I can speak ultimately to where the administration position is, but I have stated before that I think it would be helpful in certain instances if the FISA court needed additional assistance or briefing on a complicated interpretation, that they'd be able to tap such a panel, and your bill would provide the ability for them to do so, and to hear that amicus--amicus view.

Senator King. Thank you.

I understand that one of the responsibilities that you all have at the division is oversight, and that you're developing a training program for IC personnel. Could you tell us where that stands? Is it happening? Will it--is it mandatory for all IC personnel? Does it deal with the Fourth Amendment and those kinds of principles? What's the nature of that program?

Mr. Carlin. I'm not sure I'm familiar with this specific program that you're referencing, but we do work with, for instance, the NSA in the development of training programs, particularly those programs that are on the procedures, the compliance procedures that would be ordered by the court, such as minimization procedures. We would help in the development of that curriculum. And then I know our attorneys also go and train, in particular, on those issues. And we also help provide similar training, I know, to the FBI.

Senator King. Does the IC personnel generally regularly, routinely receive training that reflects the values embodied in the First Amendment? Because this is--the business that they're in is finding that right balance on a day-to-day basis. Is this part of the entry process for somebody coming into the NSA or the FBI or the CIA?

Mr. Carlin. I'm not sure I'd have the expertise to speak writ large as to the training programs for every element of the Intelligence Community. Having spent time at the FBI, I know for the FBI, that is part of their training programs. And I know it's--these issues and issues in terms of privacy and protection of U.S. persons are definitely a part of the training program at the NSA. And I expect that each who is subject to attorney general-approved guidelines in terms of the protection and handling of U.S. person information would receive training as part of the curriculum on those protected procedures.

Senator King. Thank you.

General Taylor, you have a very important responsibility. And I, like Senator Coburn, appreciate your willingness to step forward once again, and undertake service to your country.

We spend approximately \$75 billion a year on intelligence between military and civilian. That is a lot of money. And it's increased dramatically, as you know, since September 11th. So, the role of communicating and sharing, but at the same time, not duplicating, is really essential. And I hope that you will take seriously the comments and questions of Senator Coburn. And I want to associate myself with them. And here's my question.

If you, who are starting with a blank sheet of paper to set up a system to share information among intelligence and law enforcement, would you--what would you come up with? Would it be the fusion centers, or would it be some other--some other kind of entity?

General Taylor. Well, thank you, Senator, for your comments about my returning to service. I am looking forward to working with this Committee, and certainly with our colleagues at DHS.

My sense, Senator, is--the institutions exist. It's connecting the institutions appropriately. So, I wouldn't start with a blank slate. I'd figure out where the nexus (ph) are between the institutions that are currently working these issues.

Take fusion centers, for instance. Governors--adjutant generals love them because it's all source, all hazard. And so, why not use that capacity? It's already looking at all source, all hazards to help inform the Intelligence Community, which is really the sweet spot for I&A.

And if we--if we do our job properly, we won't be duplicating any work that's done by the FBI and the JTTF. We don't do investigations, we don't do overt--we don't do clandestine collection of intelligence, we take information from our partners and try to turn it into information that's useful. And also, take information from the IC (ph) just to send it back. I should say I&A does.

If confirmed, I will be a part of that great team. But I think it's making sure that the mission is clear, the objectives are linked, and the outcomes meet the expectations of our customers and partners, as opposed to kind of doing what

we were--what we did before we came to the--to I&A, for instance. When we came out of the IC, (ph) we did it a certain way. If we came out of the FBI, we did it another way.

Senator King. Well, I understand the IG is looking at some of the activities and at the GAO report. And I hope--I think you used the term--this term, Senator Coburn, and that is ``value,' and determine the value achieved versus the cost-- what the proper cost-sharing relationship should be with the states and localities. Because--you know, every hearing I go to is--we've partially removed the cloud of sequestration for a year or so, but it's not gone. And I think it's safe to say, we're going to be in a budget-constrained attitude for some period of years. And therefore we have to constantly be thinking about how do we achieve the same or greater value at the same or lesser cost?

So, I commend that mission to you, sir.

General Taylor. Yes, sir. Well, one of my marching orders from the secretary is to do just that--to eliminate duplication where it exists, and to improve the efficiency of our mission execution within I&A. And I intend, if confirmed, to follow those instructions, as well as your instructions, sir.

Senator King. Well, if you are successful in eliminating some duplication around here, I'll put in a bill to build a statue of you in the courtyard.

[Laughter.]

Thank you very much, General.

General Taylor. Yes, sir, thank you.

Senator King. I appreciate it.

Chairman Feinstein. Thank you very much, Senator King. It looks like we will be able to make this vote.

I just want to say one thing to both of our nominees. You both occupy points of great interest to this Committee. And I will hope that you will be coming before us singly within the next six-month period.

I think, General Taylor, we really want to delve into more detail on your mission as you see it--the reduction of contractors within your organization, and the increase of fresh, bright, new intelligence. So we will do that.

Mr. Carlin, your division is very important to this Committee. It is a very vital part of the oversight role. And I think you, too, might want to give some additional thought to it, and come before the Committee. And I think we should talk a little bit about it.

And I see a very beautiful young lady I happen to have some Senate lollipops for in the front row.

So, I'm going to say one thing about questions from the Members. We'd like to have them in by close of business on Friday so that we can move--take our vote and move these nominees as soon as possible. If we get them in, we'll schedule the vote for next week.

So, thank you both. Thank you, ladies and gentlemen. And the hearing is adjourned.

[Whereupon, at 5:53 p.m., the Committee adjourned.]

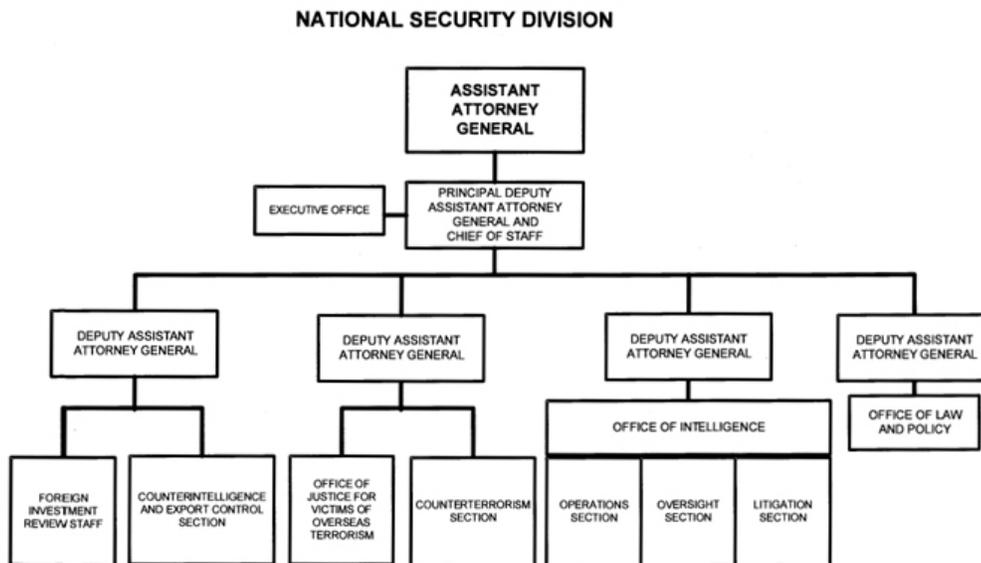
Supplemental Material

[GRAPHICS NOT AVAILABLE IN TIFF FORMAT]

[all]

Exhibit 22

ORGANIZATION, MISSION AND FUNCTIONS MANUAL: NATIONAL SECURITY DIVISION



Approved by  Date: Jan. 7, 2015
ERIC H. HOLDER, JR.
 Attorney General

d

The National Security Division (NSD) was created in March 2006 by the USA PATRIOT Reauthorization and Improvement Act (Pub. L. No. 109-177). The creation of the NSD consolidated the Justice Department’s primary national security operations: the former Office of Intelligence Policy and Review and the Counterterrorism and Counterespionage Sections of the Criminal Division. The new Office of Law and Policy and the Executive Office, as well as the Office of Justice for Victims of Overseas Terrorism (which previously operated out of the Criminal Division, complete the NSD) complete the NSD. The NSD commenced operations in September 2006 upon the swearing in of the first Assistant Attorney General for National Security.

The mission of the National Security Division is to carry out the Department’s highest priority: to combat terrorism and other threats to national security. NSD is designed to ensure greater coordination and unity of purpose between prosecutors and law enforcement agencies on the one hand, and intelligence attorneys and the Intelligence Community on the other, thus strengthening the effectiveness of the Federal Government’s national security efforts.

The National Security Division’s major responsibilities include:

Intelligence Operations and Litigation

- Ensuring that IC agencies have the legal tools necessary to conduct intelligence operations.
- Representing the United States before the Foreign Intelligence Surveillance Court (FISC) to obtain authorization under the Foreign Intelligence Surveillance Act (FISA) for government agencies to conduct intelligence collection activities;
- Coordinating and supervising intelligence-related litigation matters, including the evaluation and review of requests to use information collected under FISA in criminal and non-criminal proceedings and to disseminate FISA information; and
- Serving as the Department’s primary liaison to the Director of National Intelligence and the IC.

Counterterrorism

- Promoting and overseeing a coordinated national counterterrorism enforcement program, through close collaboration with Department leadership, the National Security Branch of the FBI, the IC, and the 94 United States Attorneys’ Offices (USAOs);
- Developing national strategies for combating emerging and evolving terrorism threats, including the threat of cyber-based terrorism;
- Overseeing and supporting the Anti-Terrorism Advisory Council (ATAC) program by:
 - 1) collaborating with prosecutors nationwide on terrorism matters, cases, and threat information;
 - 2) maintaining an essential communication network between the Department and USAOs for the rapid transmission of information on terrorism threats and investigative activity; and
 - 3) managing and supporting ATAC activities and initiatives;
- Consulting, advising, and collaborating with prosecutors nationwide on international and domestic terrorism investigations, prosecutions, and appeals, including the use of classified evidence through the application of the Classified Information Procedures Act (CIPA);

- Sharing information with and providing advice to international prosecutors, agents, and investigating magistrates to assist in addressing international threat information and litigation initiatives; and
- Managing DOJ's work on counter-terrorist financing programs, including supporting the process for designating Foreign Terrorist Organizations and Specially Designated Global Terrorists as well as staffing U.S. Government efforts on the Financial Action Task Force.

Counterespionage

- Supporting and supervising the investigation and prosecution of espionage and related cases through coordinated efforts and close collaboration with Department leadership, the FBI, the IC, and the 94 USAOs;
- Developing national strategies for combating the emerging and evolving threat of cyber-based espionage and state-sponsored cyber intrusions;
- Assisting in and overseeing the expansion of investigations and prosecutions into the unlawful export of military and strategic commodities and technology, including by assisting and providing guidance to USAOs in the establishment of Export Control Proliferation Task Forces;
- Coordinating and providing advice in connection with cases involving the unauthorized disclosure of classified information and supporting resulting prosecutions by providing advice and assistance with the application of CIPA; and
- Enforcing the Foreign Agents Registration Act of 1938 (FARA) and related disclosure statutes.

Oversight and Reporting

- Overseeing certain foreign intelligence, counterintelligence, and other national security activities of IC components to ensure compliance with the Constitution, statutes, and Executive Branch policies to protect individual privacy and civil liberties;
- Monitoring certain intelligence and counterintelligence activities of the FBI to ensure conformity with applicable laws and regulations, FISC orders, and Department procedures, including the foreign intelligence and national security investigation provisions of the Attorney General's Guidelines for Domestic FBI Operations; and
- Fulfilling statutory, Congressional, and judicial reporting requirements related to intelligence, counterintelligence, and other national security activities.

Policy and Other Legal Issues

- Handling appeals in cases involving national security-related prosecutions, and providing views on appellate issues that may impact national security in other civil, criminal, and military commissions cases;
- Providing legal and policy advice on the national security aspects of cybersecurity policy and cyber-related operational activities;
- Providing advice and support on national security issues that arise in an international context, including assisting in bilateral and multilateral engagements with foreign governments and working to build counterterrorism capacities of foreign governments and enhancing international cooperation;
- Providing advice and support on legislative matters involving national security issues, including developing and commenting on legislation, supporting Departmental engagements with members of Congress and Congressional staff, and preparing testimony for senior Division/Department leadership;
- Providing legal assistance and advice on matters arising under national security laws and policies, and overseeing the development, coordination, and implementation of Department-wide policies with regard to intelligence, counterintelligence, counterterrorism, and other national security matters; handling issues related to classification and declassification of records, records management, and freedom of information requests and related litigation; and
- Developing a training curriculum for prosecutors and investigators on cutting-edge tactics, substantive law, and relevant policies and procedures.

Foreign Investment

- Performing the Department's staff-level work on the Committee on Foreign Investment in the United States (CFIUS), which reviews foreign acquisitions of domestic entities that might affect national security and makes recommendations to the President on whether such transactions threaten the national security;
- Tracking and monitoring certain transactions that have been approved, including those subject to mitigation agreements, and identifying unreported transactions that might merit CFIUS review;
- Responding to Federal Communication Commission (FCC) requests for the Department's views relating to the national security implications of certain transactions relating to FCC licenses; and
- Tracking and monitoring certain transactions that have been approved pursuant to this process.

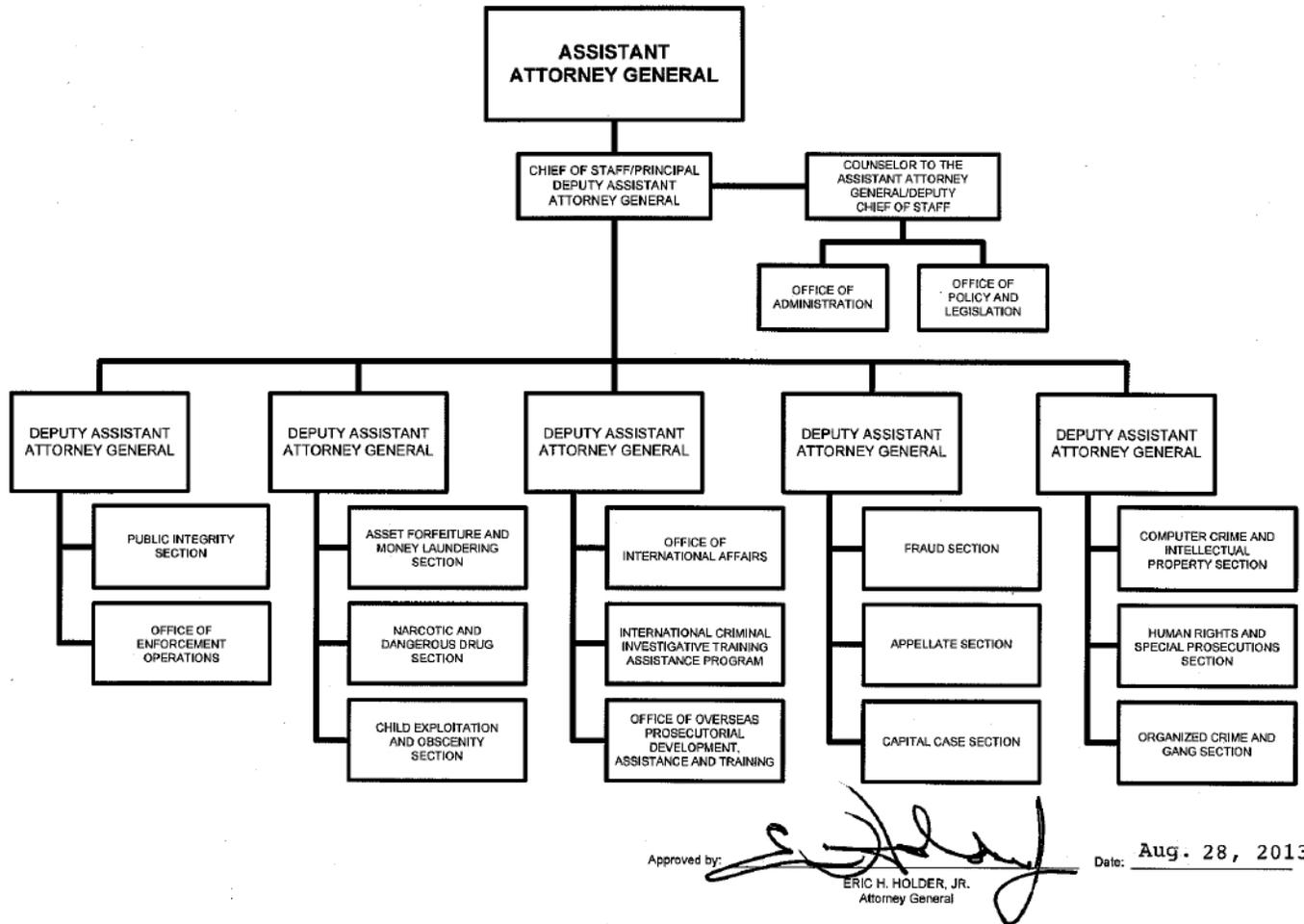
Victims of Terrorism

- Through NSD's OVT, prioritizing within the Department the investigation and prosecution of terrorist attacks that have resulted in the deaths and/or injuries of American citizens overseas; and
- Ensuring that the rights of victims and their families are honored and respected, and that victims and their families are supported and informed during the criminal justice process.

[Return to the table of contents](#)

Exhibit 23

ORGANIZATION, MISSION AND FUNCTIONS MANUAL: CRIMINAL DIVISION



d

The Criminal Division was created by Attorney General Palmer in his reorganization of the Department of Justice in 1919.

The mission of the Criminal Division is to serve the public interest through the enforcement of criminal statutes in a vigorous, fair, and effective manner; and to exercise general supervision over the enforcement of all federal criminal laws, with the exception of those statutes specifically assigned to the Antitrust, Civil Rights, Environment and Natural Resources, or Tax Divisions.

The major functions of the Division are to:

- Develop, enforce, and supervise the application of all federal criminal laws, except those specifically assigned to other divisions of the Department.
- Supervise a wide range of criminal investigations and prosecutions, including international and national drug trafficking and money laundering organizations; international organized crime groups; corrupt public officials; human rights violators; domestic and international child exploitation enterprises; domestic and international hackers; and individuals and organizations responsible for financial fraud and misconduct.
- Approve and oversee the use of the most sophisticated investigative authorities in the federal arsenal, including reviewing all federal electronic surveillance requests in criminal cases and authorizing participation in the Witness Security Program.
- Advise the Attorney General and other senior leadership within the Executive Branch on matters of criminal law.
- Coordinate with foreign countries to secure the return of fugitives and obtain evidence and other assistance from abroad, and assure that the United States meets its reciprocal obligations to treaty partners.
- Formulate and implement criminal enforcement policy and provide advice and assistance to all levels of the law enforcement community, including providing training to federal, state, and local prosecutors and investigative agencies.
- Provide training and development assistance to foreign criminal justice systems.

The Division's major responsibilities include:

- Public integrity – Identifying, investigating, and prosecuting corrupt government officials; providing expertise, guidance, and instruction to law enforcement agents and prosecutors on matters involving corruption; and ensuring that sensitive public corruption and election crime matters are handled in a uniform, consistent, and appropriate manner across the country.

- Human rights and special prosecutions – Investigating and prosecuting cases related to human rights violations, international violent crime, and complex immigration crimes; pursuing the U.S. Government's commitment to holding accountable human rights violators and war criminals, both as a domestic law enforcement imperative and as a contribution to the global effort to end impunity.
- Fraud - Investigating and prosecuting sophisticated and multi-district white-collar crimes including corporate, securities, and investment fraud, government program and procurement fraud, health care fraud, and international criminal violations including the bribery of foreign government officials in violation of the Foreign Corrupt Practices Act.
- Child exploitation - Prosecuting high-impact cases involving online child pornography, the online grooming and inducement of children by sexual predators, sex trafficking of children, travel abroad by U.S. citizens and residents to sexually abuse foreign children (sex tourism), and enforcement of sex offender registration laws; providing forensic assistance to federal prosecutors and law enforcement agents in investigating and prosecuting violations of federal criminal statutes criminalizing child exploitation; coordinating nationwide operations targeting child predators; and developing policy and legislative proposals related to these issues.
- Computer crime and intellectual property crime - Working to prevent and respond to criminal cyber attacks; improving the domestic and international laws to most effectively prosecute computer and IP criminals; and directing multi-district and transnational cyber investigations and prosecutions.
- Narcotics and dangerous drugs - Combating domestic and international drug trafficking and narco-terrorism; drawing on available intelligence to prosecute individuals and criminal organizations posing the most significant drug trafficking threat to the United States; enforcing laws that criminalize the extraterritorial manufacture or distribution of controlled substances intended for the United States; and facilitating the provision of targeted intelligence support to DEA and other law enforcement agencies worldwide.
- Organized crime – Overseeing the Department's program to combat organized crime by: investigating and prosecuting nationally and internationally significant organized crime organizations and gangs; exercising approval authority over all proposed federal prosecutions under the Racketeer Influenced and Corrupt Organizations (RICO) and Violent Crimes in Aid of Racketeering (VICAR) statutes; supporting criminal prosecutions of federal crimes involving labor-management disputes, the internal affairs of labor unions in the private sector, and the operation of employee pension and welfare benefit plans; working with U.S. intelligence agencies and U.S. and foreign law enforcement agencies to identify, target, and investigate transnational organized crime groups; and contributing to the development of policy and legislation relating to numerous organized crime-related issues, including gambling and human trafficking.
- Sensitive investigative techniques - Overseeing the use of the most sophisticated investigative tools at the Department's disposal; reviewing federal electronic and video surveillance requests; authorizing participation in the Federal Witness Security Program; and reviewing requests for witness immunity, transfers of prisoners to and from foreign countries to serve the remainder of their prison sentences, attorney and press subpoenas, applications for S-Visa status, and the imposition of special administrative measures to further restrict the confinement conditions of certain very dangerous persons in the custody of the Bureau of Prisons.
- International affairs - Making all requests for international extraditions and for foreign evidence on behalf of federal, state, and local prosecutors and investigators; satisfying foreign requests for fugitives and evidence located in the U.S.; negotiating and implementing law enforcement treaties; providing guidance to prosecutors and investigators on legal and policy issues arising in sensitive transnational investigations; and providing critical advice to the Attorney General and other principals of the Department on matters involving international law enforcement cooperation and comparative criminal law and practice.
- Assistance to foreign law enforcement institutions (police and corrections) - Supporting the creation and development of new and existing police forces in other countries and international peacekeeping operations; enhancing the capabilities of existing police forces in emerging democracies; strengthening U.S. national security by assisting nations that are on the front lines of the war on terrorism, and creating sustainable foreign law enforcement institutions that promote democratic principles, instill respect for human rights and human dignity, and reduce the threat of transnational crime and terrorism.
- Policy and legislation - Serving as subject matter experts in all matters relating to criminal law and using that expertise to develop legislative and policy proposals to enhance our ability to fight crime; serving as the Department representative to the U.S. Sentencing Commission.
- Appeals - Drafting briefs and certiorari petitions for the Solicitor General for filing in the U.S. Supreme Court; making recommendations to the Solicitor General as to whether further review is warranted on adverse criminal decisions in the district courts and courts of appeals; and preparing briefs and arguing cases in the courts of appeals.
- Capital cases - Advising on factual and legal issues relevant to capital eligible cases and decisions to seek the death penalty; providing legal, procedural, and policy guidance and direct litigation support to United States Attorney's Offices handling capital investigations and prosecutions.
- Money laundering and asset recovery - Pursuing criminal prosecutions against financial institutions and individuals engaged in money laundering, Bank Secrecy Act, and sanctions violations; pursuing the proceeds of high level foreign corruption through the Kleptocracy Asset Recovery Initiative; developing legislative, regulatory, and policy initiatives to combat global illicit finance; returning forfeited criminal proceeds to benefit those harmed by crime through remission and restoration processes; and providing legal and policy assistance and training to federal, state, and local prosecutors and law enforcement personnel, as well as to foreign governments.

[Return to the table of contents](#)

Updated September 2, 2016

Exhibit 24



Office of the Attorney General
Washington, D. C. 20530
May 10, 2017

MEMORANDUM FOR ALL FEDERAL PROSECUTORS

FROM: THE ATTORNEY GENERAL 
SUBJECT: Department Charging and Sentencing Policy

This memorandum establishes charging and sentencing policy for the Department of Justice. Our responsibility is to fulfill our role in a way that accords with the law, advances public safety, and promotes respect for our legal system. It is of the utmost importance to enforce the law fairly and consistently. Charging and sentencing recommendations are crucial responsibilities for any federal prosecutor. The directives I am setting forth below are simple but important. They place great confidence in our prosecutors and supervisors to apply them in a thoughtful and disciplined manner, with the goal of achieving just and consistent results in federal cases.

First, it is a core principle that prosecutors should charge and pursue the most serious, readily provable offense. This policy affirms our responsibility to enforce the law, is moral and just, and produces consistency. This policy fully utilizes the tools Congress has given us. By definition, the most serious offenses are those that carry the most substantial guidelines sentence, including mandatory minimum sentences.

There will be circumstances in which good judgment would lead a prosecutor to conclude that a strict application of the above charging policy is not warranted. In that case, prosecutors should carefully consider whether an exception may be justified. Consistent with longstanding Department of Justice policy, any decision to vary from the policy must be approved by a United States Attorney or Assistant Attorney General, or a supervisor designated by the United States Attorney or Assistant Attorney General, and the reasons must be documented in the file.

Second, prosecutors must disclose to the sentencing court all facts that impact the sentencing guidelines or mandatory minimum sentences, and should in all cases seek a reasonable sentence under the factors in 18 U.S.C. § 3553. In most cases, recommending a sentence within the advisory guideline range will be appropriate. Recommendations for sentencing departures or variances require supervisory approval, and the reasoning must be documented in the file.

Memorandum for All Federal Prosecutors
Subject: Department Charging and Sentencing Policy

Page 2

Any inconsistent previous policy of the Department of Justice relating to these matters is rescinded, effective today.¹

Each United States Attorney and Assistant Attorney General is responsible for ensuring that this policy is followed, and that any deviations from the core principle are justified by unusual facts.

I have directed the Deputy Attorney General to oversee implementation of this policy and to issue any clarification and guidance he deems appropriate for its just and consistent application.

Working with integrity and professionalism, attorneys who implement this policy will meet the high standards required of the Department of Justice for charging and sentencing.

¹ Previous policies include: *Department Policy on Charging Mandatory Minimum Sentences and Recidivist Enhancements in Certain Drug Cases* (August 12, 2013); and *Guidance Regarding § 851 Enhancements in Plea Negotiations* (September 24, 2014).

Exhibit 25

2901331



Office of the Attorney General
Washington, D. C. 20530

September 24, 2014

TO: DEPARTMENT OF JUSTICE ATTORNEYS
FROM: *EX* THE ATTORNEY GENERAL
RE: Guidance Regarding § 851 Enhancements In Plea Negotiations

2014 SEP 24 PM 3:46
DEPT. OF JUSTICE
EXECUTIVE SECRETARIAT

The Department of Justice's charging policies are clear that in all cases, prosecutors must individually evaluate the unique facts and circumstances and select charges and seek sentences that are fair and proportional based upon this individualized assessment. "Department Policy on Charging and Sentencing," May 10, 2010. The Department provided more specific guidance for charging mandatory minimums and recidivist enhancements in drug cases in the August 12, 2013, "Department Policy on Charging Mandatory Minimum Sentences and Recidivist Enhancements in Certain Drug Cases." That memorandum provides that prosecutors should decline to seek an enhancement pursuant to 21 U.S.C. § 851 unless the "defendant is involved in conduct that makes the case appropriate for severe sanctions," and sets forth factors that prosecutors should consider in making that determination. Whether a defendant is pleading guilty is not one of the factors enumerated in the charging policy. Prosecutors are encouraged to make the § 851 determination at the time the case is charged, or as soon as possible thereafter. An § 851 enhancement should not be used in plea negotiations for the sole or predominant purpose of inducing a defendant to plead guilty. This is consistent with long-standing Department policy that "[c]harges should not be filed simply to exert leverage to induce a plea, nor should charges be abandoned to arrive at a plea bargain that does not reflect the seriousness of the defendant's conduct." "Department Policy on Charging and Sentencing," May 19, 2010.

While the fact that a defendant may or may not exercise his right to a jury trial should ordinarily not govern the determination of whether to file or forego an § 851 enhancement, certain circumstances -- such as new information about the defendant, a reassessment of the strength of the government's case, or recognition of cooperation -- may make it appropriate to forego or dismiss a previously filed § 851 information in connection with a guilty plea. A practice of routinely premising the decision to file an § 851 enhancement solely on whether a defendant is entering a guilty plea, however, is inappropriate and inconsistent with the spirit of the policy.

Exhibit 26

ACLU v. DOJ, 13 Civ. 7347 (S.D.N.Y.)
Documents Withheld in Full by National Security Division, August 2015

Doc. No.	Date	From/To	Pages	Subject/Description	Exemption/Privilege
1.	undated	National Security Division (unnamed author); no recipient specified	1	Segment of internal Executive Branch memo captioned “FISA versus Traditional Law Enforcement Warrants.” Informal form (e.g., no letterhead, no identification of sender or recipient). Provides legal advice on questions, including whether information is FISA-derived in certain contexts. Memo was prepared in anticipation of litigation and discusses issues for prosecutors’ consideration.	(b)(5): deliberative process privilege; work product; attorney-client privilege
2.	undated	National Security Division (unnamed author); no recipient specified	1	Segment of untitled internal Executive Branch memo providing legal advice on the meaning of “derived” and whether evidence should be considered “derived.” Informal form (e.g., no letterhead, no identification of sender or recipient). Prepared in anticipation of litigation. Memo was prepared in anticipation of litigation and discusses issues for prosecutors’ consideration.	(b)(5): deliberative process privilege; work product; attorney-client privilege
3.	2011-2013	National Security Division (unnamed author); no recipient specified	Varies	Multiple Drafts of an internal Executive Branch memo titled, “Memorandum of Law in Support of Guidance Regarding Whether Information is Derived from FISA.” Memo provides legal analysis of FISA and its history, use of FISA-obtained and FISA-derived information in proceedings, scope of “derived” evidence, and FISA use practice in various scenarios; advises prosecutors on applying principles regarding whether information is FISA-derived. Memo was prepared in anticipation of litigation and discusses issues for prosecutors’ consideration.	(b)(5): deliberative process privilege; work product; attorney-client privilege

4.	undated	National Security Division (unnamed author); no recipient specified	3	Untitled internal Executive Branch memo setting forth and evaluating arguments regarding the meaning of derived from FISA. Informal form (e.g., no letterhead, no identification of sender or recipient). Memo was prepared in anticipation of litigation and discusses issues for prosecutors' consideration.	(b)(5): deliberative process privilege; work product; attorney-client privilege
5.	undated	Office of the Director of National Intelligence (ODNI), Office of General Counsel; no recipient specified	1	Note from ODNI's Office of the General Counsel (OGC) titled "FISA-Derived Views," regarding ODNI's approach to the FISA-derived issue and history and progress of interagency discussions. Informal form (e.g., no letterhead, no identification of sender or recipient). Informally expresses ODNI's views in advance of consultative meeting, expresses issues of concern to various agencies, recommends positions, and hopes for discussion of certain issues. Memo was prepared in anticipation of litigation.	(b)(5): deliberative process privilege; work product; attorney-client privilege
6.	undated	National Security Division, Office of Intelligence; no recipient specified	2	Internal Executive Branch memo titled "FISA Derived Additional Views," regarding the drafting of FISA-derived policy guidance, setting forth views on appropriate scope of future guidance, and discussing legal issues related to that guidance. Informal form (e.g., no letterhead, no identification of sender or recipient). Part of consultative process, making recommendation regarding how to proceed on guidance document. Memo was prepared in anticipation of litigation and discusses issues for prosecutors' consideration.	(b)(5): deliberative process privilege; work product; attorney-client privilege
7.	July 2006 to Jan 2008	Three United States Attorneys; no recipient specified	6	Internal Executive Branch memo titled "USAO Views on FISA Use and FISA Derived," setting forth views of three United States Attorneys on various dates regarding interpretations of FISA use and FISA-derived and effects on litigation. Informal form (e.g., no letterhead, no identification of sender or recipient); informal discussion (dialogue format). Memo was prepared in anticipation of litigation and discusses issues for prosecutors' consideration.	(b)(5): deliberative process privilege; work product; attorney-client privilege

8.	Sept 26, 2008	National Security Division; no recipient specified (“to” and “from” fields in memo blank)	7	Draft Executive Branch Memo titled, “Guidance Regarding Information Derived From FISA Collection,” providing guidance on issues related to information derived from FISA collection and illustrative examples. Memo is saved with a file name which includes the date, but memo itself is dated “October __, 2008.” Memo was prepared in anticipation of litigation and discusses issues for prosecutors’ consideration.	(b)(5): deliberative process privilege; work product; attorney-client privilege
9.	Oct 14, 2008	Assistant Attorney General for National Security Patrick Rowan /All Federal Prosecutors	8	Another draft of document 8. Memo is saved with a file name which includes the date, but memo itself is dated “October __, 2008.”	(b)(5): deliberative process privilege; work product; attorney-client privilege
10.	2010-2012	Attorney General Eric Holder /All Federal Prosecutors	Varies	Multiple Drafts of an Executive Branch memo titled, “Guidance Regarding Whether Information Is ‘Derived From’ FISA.” Memo is not on letterhead, but there is a note to place it on letterhead. Memo provides legal advice to prosecutors on when information is “derived from” FISA Surveillance. Memo is saved with a file name that has a date, but memo itself is undated. Memo was prepared in anticipation of litigation and discusses issues for prosecutors’ consideration.	(b)(5): deliberative process privilege; work product; attorney-client privilege
11.	2011-2012	National Security Division/no recipient specified	Varies	Multiple Drafts of an Executive Branch memo titled, “Addendum to the Guidance Regarding How to Determine Whether Information is ‘Derived From’ FISA Surveillance” Memo includes illustrative case examples on whether information is FISA derived for use by Federal prosecutors and federal agents. Memo is saved with a file name that has a date, but memo itself is undated. Memo was prepared in anticipation of litigation and discusses issues for prosecutors’ consideration.	(b)(5): deliberative process privilege; work product; attorney-client privilege

12.	2013-2014	National Security Division/no recipient specified	Varies	Multiple Drafts of a Redlined Executive Branch Memo marked "Draft" and "Attorney Work Product," titled, "Determining Whether Evidence Is 'Derived From' Surveillance Under Title III or FISA," which provides legal advice on whether evidence is derived from surveillance under FISA or Title III. Memo is not on letterhead. There are no "To" or "From" fields. Memo was prepared in anticipation of litigation and discusses issues for prosecutors' consideration. Various drafts contain revisions made by the Criminal Division.	(b)(5): deliberative process privilege; work product; attorney-client privilege
13.	June 17, 2013	National Security Division/ National Security Division	16	Draft internal Executive Branch "memorandum to the file" from a National Security Division attorney discussing the use of FISA information in notice proceedings. Memo was saved with a file name that included a date, but the memo itself is dated, "May ___, 2013." The memo is watermarked "Draft" and was prepared in anticipation of litigation and discusses issues for government attorneys' consideration.	(b)(5): deliberative process privilege; work product; attorney-client privilege
14.	June 24, 2013	National Security Division/no recipient specified	24	Executive Branch memo watermarked "Draft" and marked "Confidential" and "Attorney-Client Work Product" which provides legal advice on when information is derived from FISA. Memo is not on letterhead, is not titled, and there are no "To" or "From" fields. Memo is saved with a file name which includes a date, but the memo itself is undated. Memo was prepared in anticipation of litigation and discusses issues for prosecutors' consideration.	(b)(5): deliberative process privilege; work product; attorney-client privilege

15.	June 24, 2013	National Security Division/no recipient specified	6	Draft Executive Branch memorandum which analyzes when information is “derived from” FISA surveillance. Memo is not on letterhead; it is not titled, and there are no “To” and “From” fields. Memo is saved with a file name which includes a date, but the memo itself is undated. Memo was prepared in anticipation of litigation and discusses issues for prosecutors’ consideration.	(b)(5): deliberative process privilege; work product; attorney-client privilege
16.	July 8, 2013	National Security Division	9	Draft Executive Branch memorandum which analyzes when information is “derived from” FISA surveillance. Memo is not on letterhead; it is not titled, and there are no “To” and “From” fields. Memo is saved with a file name which includes a date, but the memo itself is undated. Memo was prepared in anticipation of litigation and discusses issues for prosecutors’ consideration. Draft of document #5 in Feb. 2014 index of withheld documents.	(b)(5): deliberative process privilege; work product; attorney-client privilege
17.	July 3, 2013	National Security Division	9	Another draft of document 16. (Draft of document #5 in Feb. 2014 index of withheld documents).	(b)(5): deliberative process privilege; work product; attorney-client privilege
18.	July 15, 2013	National Security Division/no recipient specified	7	Draft Executive Branch memorandum which analyze when information is “derived from” FISA surveillance and how to properly satisfy FISA’s statutory notice obligation. Memo is not on letterhead; it is not titled, and there are no “To” and “From” fields. Memo was prepared in anticipation of litigation and discusses issues for prosecutors’ consideration. Draft of document #2 in Feb. 2014 index of withheld documents.	(b)(5): deliberative process privilege; work product; attorney-client privilege

19.	July 15, 2013	Office of the Solicitor General/no recipient specified	6	Document #1 in Feb. 2014 index of withheld documents, attached to cover email to federal executive branch employees.	(b)(5): deliberative process privilege; work product; attorney-client privilege
20.	July 16, 2013	National Security Division/no recipient specified	5	Draft Executive Branch memorandum which analyzes when information is “derived from” FISA surveillance and how to properly satisfy FISA’s statutory notice obligation. Memo is not on letterhead; it is not titled, and there are no “To” and “From” fields. Memo is saved with a file name that includes the date, but memo itself is undated. Memo was prepared in anticipation of litigation and discusses issues for prosecutors’ consideration. Draft of document #2 in Feb. 2014 index of withheld documents.	(b)(5): deliberative process privilege; work product; attorney-client privilege
21.	Sept 10, 2013	National Security Division/no recipient specified	14	Internal Executive Branch memo titled, “Memorandum of Law in Support of Guidance Regarding Whether Information is Derived from FISA.” Memo is marked “Draft.” Provides legal analysis of FISA and its history, use of FISA-obtained and FISA-derived information in proceedings, scope of “derived” evidence, and FISA use practice in various scenarios; advises prosecutors on applying principles regarding whether information is FISA-derived. Memo was prepared in anticipation of litigation and discusses issues for prosecutors’ consideration.	(b)(5): deliberative process privilege; work product; attorney-client privilege
22.	Sept 16, 2013	Office of the Solicitor General/no recipient specified	15	Executive Branch Memo marked “Draft” which discusses when evidence is derived from surveillance under FISA. Memo is not on letterhead. Memo is saved with a file name that includes the date, but the memo itself is dated September [], 2013. Memo was prepared in anticipation of litigation and discusses issues for prosecutors’ consideration.	(b)(5): deliberative process privilege; work product; attorney-client privilege

23.	Oct 14, 2013	Office of the Solicitor General/no recipient specified	18	Another draft of document 22. Memo is saved with a file name that includes the date, but the memo itself is dated October [], 2013.	(b)(5): deliberative process privilege; work product; attorney-client privilege
24.	Nov 14, 2013	Office of the Solicitor General/no recipient specified	4	Redlined Executive Branch Memo marked "Draft" which addresses meaning of "derived from" FISA and includes sample scenarios. Memo is not on letterhead and contains no "To" or "From" fields. Memo was prepared in anticipation of litigation and discusses issues for prosecutors' consideration.	(b)(5): deliberative process privilege; work product; attorney-client privilege
25.	July 17, 2013	not stated	2	Draft "Summary of July 17, 2013 Meeting Concerning Interpretation of 'FISA-Derived' and Notice of Use of FISA Title VII Information in FISA Suppression Litigation." Summarizes issues for further consultation and consideration. Memo was prepared in anticipation of litigation and discusses issues for prosecutors' consideration. Draft of document #3 from Feb. 2014 index of withheld documents.	(b)(5): deliberative process privilege; work product; attorney-client privilege
26.	2014-2015	National Security Division/All Federal Prosecutors	Varies	Multiple drafts of an Executive Branch Memo marked "Attorney Work Product" and "Privileged and Confidential" which provides legal advice by discussing when evidence is derived from surveillance under FISA. Memo is not on letterhead. Memo saved with a file name that includes a date, but memo itself is dated, "_____, 2014." Memo was prepared in anticipation of litigation and discusses issues for prosecutors' consideration. Drafts contain edits from the Office of the Solicitor General.	(b)(5): deliberative process privilege; work product; attorney-client privilege

27.	March 4, 2015	National Security Division	3	Draft Redlined Executive Branch Memo which addresses the FISA notice requirement in certain proceedings. Memo is saved with a file name which includes the date, but the memo itself is undated. The memo is untitled, and there are no "To" or "From" fields. Memo was prepared in anticipation of litigation and discusses issues for prosecutors' consideration.	(b)(5): deliberative process privilege; work product; attorney-client privilege
28.	March 4, 2015	National Security Division	2	Another draft of document 27. Memo is saved with a file name which includes the date, but the memo itself is undated.	(b)(5): deliberative process privilege; work product; attorney-client privilege
29.	Aug 28, 2014	Department of Treasury/File	13	Executive Branch Memo which addresses the FISA notice requirement in certain proceedings. Memo is marked "Privileged" and "Draft – Predecisional and Deliberative." Memo discusses issues for government attorneys' consideration.	(b)(5): deliberative process privilege; work product; attorney-client privilege
30.	June 12, 2014	National Security Division/File	12	Executive Branch Memo which addresses the FISA notice requirement in certain proceedings. Memo is marked "Privileged and Confidential" and "Draft." Memo discusses issues for government attorneys' consideration.	(b)(5): deliberative process privilege; work product; attorney-client privilege
31.	Nov 2013	National Security Division/No recipient specified	6	Executive Branch Memo which addresses the FISA notice requirement in certain proceedings. Memo is marked draft. Memo was prepared in anticipation of litigation and discusses issues for government attorneys' consideration. Memo is saved with a file name which includes the month and year, but the memo itself is undated. Memo is classified pursuant to Executive Order 13526.	(b)(5): deliberative process privilege; work product; attorney-client privilege

32.	July 7, 2014	National Security Division/No recipient specified	4	Executive Branch Memo which addresses the FISA notice requirement in certain proceedings. Memo is not addressed to anyone. Memo was prepared in anticipation of litigation and discusses issues for government attorneys' consideration. Memo is classified pursuant to Executive Order 13526.	(b)(5): deliberative process privilege; work product; attorney-client privilege
33.	Undated	National Security Division/No recipient specified	4	Executive Branch Memo which addresses the FISA notice requirement in certain proceedings. Memo is marked draft. Memo was prepared in anticipation of litigation and discusses issues for government attorneys' consideration. Memo is undated, but it was emailed on April 1, 2014 which means it was drafted before that date. Memo is classified pursuant to Executive Order 13526.	(b)(1); (b)(5): deliberative process privilege; work product; attorney-client privilege
34.	Undated	National Security Division/No recipient specified	6	Executive Branch Memo which addresses the FISA notice requirement in certain proceedings. Memo is not addressed to anyone. Memo was prepared in anticipation of litigation and discusses issues for government attorneys' consideration.	(b)(5): deliberative process privilege; work product; attorney-client privilege
35.	April 14, 2014	National Security Division/File	7	Executive Branch Memo which addresses the FISA notice requirement in certain proceedings. Memo was prepared in anticipation of litigation and discusses issues for government attorneys' consideration. Memo is classified pursuant to Executive Order 13526.	(b)(1); (b)(5): work product; attorney-client privilege
36.	Nov 12, 2013	National Security Division/File	16	Executive Branch Memo which addresses the FISA notice requirement in certain proceedings. Memo is marked "For Official Use Only – Privileged and Confidential." Memo discusses issues for government attorneys' consideration.	(b)(5): work product; attorney-client privilege
37.	March 26, 2009	National Security Division/ National Security Division	12	Executive Branch Memo which addresses the FISA notice requirement in certain proceedings. Memo is marked "For Official Use Only – Privileged and Confidential." Memo discusses issues for government attorneys' consideration.	(b)(5): work product; attorney-client privilege

Exhibit 27

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

AMERICAN CIVIL LIBERTIES UNION,
and
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION,

Plaintiff,

v.

UNITED STATES DEPARTMENT OF
JUSTICE,

Defendant.

Civil Action No. 13-cv-7347 (GHW)

DECLARATION OF MARK A. BRADLEY

I, Mark A. Bradley, declare as follows:

1. I am the Director of the Freedom of Information Act (“FOIA”) and Declassification Unit (“NSD FOIA”) of the Office of Law and Policy in the National Security Division (“NSD”) of the United States Department of Justice (“DOJ” or “Department”). NSD is a component of the Department. NSD formally began operations on October 2, 2006, by, *inter alia*, consolidating the resources of the Department’s Office of Intelligence Policy and Review (“OIPR”)¹ and the Counterterrorism Section (“CTS”) and Counterespionage Section (“CES”) of the Department’s Criminal Division. In general, NSD handles the DOJ’s national security operations, including prosecutorial, law-enforcement, and intelligence functions. Further, I have been designated by the Attorney General of the United States as an original classification

¹ OIPR is now known as the Office of Intelligence (“OI”).

authority and a declassification authority pursuant to Executive Order 13526, §§ 1.3 and 3.1.

The statements contained in this declaration are based upon my personal knowledge, information provided to me in the course of my official duties, and determinations I have made following a review of NSD's responsive records. I make this declaration based on my personal knowledge and information provided to me in my official capacity.

2. In a letter dated, March 29, 2013, plaintiff, the American Civil Liberties Union ("ACLU") requested the following:

- (1) The case name, docket number, and court of all legal proceedings, including criminal prosecutions, current or past, in which the Department of Justice intends or intended to enter into evidence, or otherwise used or disclosed in any trial, hearing, or other proceeding, any information obtained or derived from electronic surveillance pursuant to the authority of the FAA.
- (2) Policies, procedures, and practices governing the provision of notice to "aggrieved persons," as set forth in 50 U.S.C. § 1881e(a) and § 1806(c), of the government's intent to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding information obtained or derived from electronic surveillance pursuant to the authority of the FAA.
- (3) Legal memoranda or opinions addressing or interpreting the FAA's notice provision or requirements, as set forth in 50 U.S.C. § 1881e(a) and § 1806(c).

ACLU also requested a fee waiver and expedited processing. NSD FOIA received this request on April 9, 2013.

3. NSD's response to this request was addressed by this Court in its Opinion and Order dated March 3, 2015. In sum: before that opinion and order, NSD conducted a search and identified five responsive documents, withholding all five under FOIA Exemption 5. The Court held that "DOJ improperly limited its search under Part 3 of the ACLU's request by reading the

word ‘governing’ into the request where it had not been written. DOJ is ordered to conduct a new search without the improperly-added limiting term and to release any responsive records that do not fall under a FOIA exemption.” As for any remaining issues concerning the search, the Court held that the “scope and conduct of the search” was “proper” and “reasonable.” The Court further held that the government was entitled to withhold the five identified records under FOIA’s exemptions.

4. By order of this Court, NSD FOIA conducted another search for materials that were non-governing. NSD FOIA staff met with NSD’s Deputy Assistant Attorney General for Law and Policy and the Chief of the Office of Intelligence’s Litigation Section. The Office of Law and Policy develops and implements Department of Justice policies with regard to intelligence, counterterrorism, and other national security matters and provides legal assistance and advice on matters of national security law. The Deputy Assistant Attorney General for the Office of Law and Policy confirmed that attorneys in the Office of Law and Policy had worked on FISA litigation projects that may have addressed the subject of the request. In addition, among its other duties, the Litigation Section reviews and prepares requests for Attorney General authorization to use FISA information in criminal and non-criminal proceedings. OI’s Litigation Section Chief is familiar with OI’s files, has a keen understanding of OI’s activities, and is familiar with NSD’s and OI’s practices, policies, and procedures regarding the notification requirements under FISA and the FAA. Because of this, she knew precisely which attorneys would have responsive records in their files.

5. Each of these knowledgeable component heads identified the attorneys in their sections who were responsible for drafting, editing, and maintaining records of the effort to draft

the NSD policy on FISA use. There were four attorneys in the Office of Law and Policy and two attorneys in the Litigation Section with responsive records. All six of these attorneys stated that they were responsible for distributing updated drafts to their colleagues. All of the non-governing draft materials were preserved in their electronic mail accounts and were not located in any of their other files. NSD FOIA searched the electronic mail accounts of those six attorneys and located the responsive records, specifically searching for records from the date of the passage of the FAA (July 10, 2008) to the date of the order (March 3, 2015). NSD FOIA then reviewed those records to confirm responsiveness and processed them. Upon reviewing and processing those records, NSD FOIA determined that all of them should be withheld in full.²

6. On August 21, 2015, NSD submitted a *Vaughn* index that included thirty-seven entries, which described the records NSD located in its searches for responsive documents. NSD withheld all of these documents in full. The index is attached to, and made a part of, this declaration. ACLU is challenging the withholding of thirty-one of those documents. ACLU is not challenging the withholding of six documents which are listed as numbers 8, 16, 17, 18, 20, and 25 in NSD's August 2015 *Vaughn* index.

Exemption 1

7. FOIA exemption (b)(1), 5 U.S.C. § 552(b)(1), provides that the FOIA disclosure provisions do not apply to matters that are:

² I have been informed by attorneys in Office of Law and Policy that the Department has for some time considered producing a guidance document for Department prosecutors to address certain issues concerning what information could be considered to be 'derived from' electronic surveillance under FISA, such that notice to an aggrieved person of the use of such information in a proceeding may be required. As of the date of this document, that guidance has not been completed and finalized. Drafts of such guidance exist, as well as documents commenting on the drafts, but the Department continues to deliberate as to the final form and content of the guidance document, in the event a decision is made to issue it. Accordingly, the FISA-Derived Guidance is not in final form, and all versions of the guidance are in draft form.

- (A) Specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign policy and
- (B) are in fact properly classified pursuant to such Executive Order.

8. Section 1.1 (a) of Executive Order (“E.O.”) 13526 provides that information may be originally classified under the terms of this order only if all of the following conditions are met:

- (1) an original classification authority is classifying the information;
- (2) the information is owned by, produced by or for, or is under the control of the U.S. Government;
- (3) the information falls within one or more of the categories of information listed in section 1.4 of E.O. 13526; and (4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in some level of damage to the national security and the original classification authority is able to identify or describe the damage.

9. In this case, documents 33 and 35 are properly classified. Information contained in these documents is owned by and under the control of the United States Government. The withheld information is classified TOP SECRET. Section 1.2 (a)(1) of E.O. 13526 states: “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 that the original classification authority is able to identify or describe. Section 1.4 of E.O. 13526 identifies the types of information that may be considered for classification. Of relevance to the information withheld here, the provision states that: Information shall not be considered for classification unless its unauthorized disclosure could reasonably be expected to cause identifiable or

describable damage to the national security ... and it pertains to: ... (c) intelligence activities (including covert action), intelligence sources or methods, or cryptology.

10. Here, the responsive, classified materials relate to intelligence activities, sources, or methods. Disclosure of this information would reveal information about U.S. intelligence gathering methods. Disclosure of this information would provide our adversaries and foreign intelligence targets with insight into the targets of the United States Government's foreign intelligence surveillance which in turn could be used to evade surveillance. For these reasons, the information in the withheld material is currently and properly classified pursuant to Sections 1.4 (a), (c), and (d) of E.O. 13526, and is therefore exempt from disclosure under FOIA Exemption (b)(1).

Exemption 5

11. All of the NSD records listed in the August 2015 *Vaughn* index are exempt from disclosure pursuant to FOIA Exemption 5. FOIA Exemption 5 protects "inter-agency or intra-agency memorandums or letters which would not be available by law or to a party other than an agency in litigation with the agency." 5 U.S.C. § 552(b)(5). This exemption protects documents that would normally be privileged in the civil discovery context.

12. Among the privileges incorporated into Exemption 5 is the work product privilege, which protects documents prepared as part of, or in reasonable anticipation of, litigation. The purpose of the privilege is to protect the adversarial process by insulating the attorney's preparation of litigation materials, and the mental impressions, conclusions, opinions, or theories of an attorney or other representative of a party concerning litigation.

13. In this case, all of the documents listed in NSD's *Vaughn* index are memoranda

that were prepared by Government attorneys in reasonable anticipation of litigation.³ These materials were all prepared in anticipation of possible criminal prosecutions or other adjudications. The memoranda all address how to determine if information has been derived from FISA for use in criminal prosecutions or other adjudications and the application of FISA's notice provision in those proceedings, and set out the conclusions, opinions, and legal theories of their authors in anticipation of positions to be taken in use in criminal prosecutions or other adjudications. Because all of these memoranda would be protected in civil discovery pursuant to the work product privilege, they are protected from disclosure by FOIA Exemption 5.

14. In addition, all of the records in NSD's *Vaughn* index except for items 35, 36, and 37 are also protected by Exemption 5 under the deliberative process privilege, whose purpose is to prevent injury to the quality of agency decision-making. Thus, material that contains or was prepared in connection with the formulation of opinions, advice, evaluations, deliberations, policies, proposals, conclusions, or recommendations may properly be withheld. Disclosure of this type of information would have an inhibiting effect upon agency decision-making and the development of policy because it would chill full and frank discussions between agency personnel and decision-makers regarding a decision. If agency personnel know that their preliminary impressions, opinions, evaluations, or comments would be released for public consumption, they could be less candid and more circumspect in expressing their thoughts, which would impede the full discussion of issues necessary to reach a well-reasoned decision.

15. In order to invoke the deliberative process privilege, the protected information

³ NSD Document 7 is addressed in the declaration of John Kornmeier, and NSD Document 10 is addressed in the declaration of Vanessa Brinkman.

must be both “pre-decisional” and “deliberative.” Information is “pre-decisional” if it temporally precedes the decision or policy to which it relates. It is “deliberative” if it played a direct part in the decision-making process because it consists of recommendations or opinions on legal or policy matters, or reflects the give-and-take of the consultative process.

16. In this case, NSD’s records 1-6, 9, 11-15, 19, 21-24, and 26-34 are “pre-decisional.” All of these documents are drafts of memoranda that discuss how to determine if information is derived from surveillance under the Foreign Intelligence Surveillance Act (“FISA”) or discuss compliance with FISA’s notice requirement.⁴ They are pre-decisional because they preceded a final decision regarding the government’s ultimate position on the questions they discuss. In addition, all of these documents are “deliberative” because they reflect ongoing deliberations by government attorneys regarding how to determine if information is derived from surveillance under FISA or how the government should comply with FISA’s notice requirement. The documents describe the views and recommendations of various people within the government, as part of a process to assist the government’s decision-making prior to an ultimate decision, and as part of the exchange of ideas and suggestions that accompanies careful and reasoned decision-making.

17. Reflecting and confirming their nature as deliberative and pre-decisional, many of the documents at issue are informal in their form, lacking indicia of finality such as letterhead or other headers, dates, or names or titles of the authors or recipients. As indicated in the attached index, those documents include items 1-6, 9, 11-15, 19, 21-24, and 26-34. Such informality and

⁴ Document 35 is a final, non-draft document. It is dated April 14, 2014, and NSD FOIA did not locate it in the search preceding the previous cross-motions for summary judgment because it post-dated the cut-off date for that search.

lack of indicia of final agency decision-making is characteristic of deliberative and pre-decisional records.

18. Further, all of NSD's records are also exempt under Exemption 5 pursuant to the attorney-client privilege. The attorney-client privilege concerns confidential communication between an attorney and his/her client pertaining to a legal matter for which the client has sought the attorney's counsel. This privilege's purpose is to encourage attorneys and their clients to communicate fully and honestly without fear of embarrassment and other harms. Particularly in the context of government attorneys, the privilege further serves to promote the public interest in the observance of law and the administration of justice.

19. In this case, all of the withheld materials contain legal advice, including policy advice regarding the government's best practices for implementation of its obligations, prepared by government attorneys for other government personnel who represent the client, the United States of America. The drafts of these memoranda reflect the attorneys' views on how to determine if information is derived from FISA or on how the government should comply with FISA's notice provision. These memoranda were sought by the government's decision-makers and their representatives to obtain legal advice on those issues and indeed provided such advice. The materials furthermore were intended to be, and were in fact, kept confidential—they were circulated only within the Executive Branch and accessed only by government lawyers working on the issues addressed by the memoranda. They are therefore protected by the attorney-client privilege.

20. The Department of Justice continues to deliberate as to its final conclusions regarding the issues addressed in the documents at issue here—in particular, the issue of what

information could be considered “derived from” electronic surveillance under FISA, such that notice to an aggrieved person of the use of such information in a proceeding may be required. The documents at issue here do not constitute the Department’s “working law” or “effective law and policy.” They were not provided as operative guidance to Department prosecutors, they do not have the force and effect of law within the Department, and they have not been adopted by the Department as governing policies.

CONCLUSION

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

Executed this 23rd day of November, 2015.


MARK A. BRADLEY

Exhibit 28

ORGANIZATION, MISSION AND FUNCTIONS MANUAL

Department of Justice Overview | DOJ Organizational Chart

Office of the Attorney General (AG)

Office of the Deputy Attorney General (DAG)

Office of the Associate Attorney General (ASG)

Office of the Solicitor General (OSG)

OSG Organizational Chart

Antitrust Division (ATR)

ATR Organizational Chart | ATR Field Structure Map

Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)

ATF Organizational Chart | ATF Field Structure Map

Civil Division (CIV)

CIV Organizational Chart | CIV Field Structure Map

Civil Rights Division (CRT)

CRT Organizational Chart

Community Relations Service (CRS)

CRS Organizational Chart | CRS Field Structure Map

Criminal Division (CRM)

CRM Organizational Chart

Drug Enforcement Administration (DEA)

DEA Organizational Chart | DEA Field Structure Map

Environment and Natural Resources Division (ENRD)

ENRD Organizational Chart | ENRD Field Structure Map

Executive Office for Immigration Review (EOIR)

EOIR Organizational Chart | EOIR Field Structure Map

Executive Office for Organized Crime Drug Enforcement Task Forces (OCDETF)

OCDETF Organizational Chart

Executive Office for United States Attorneys (EOUSA)

EOUSA Organizational Chart | EOUSA Field Structure Map

Executive Office for United States Trustees (EOUST)

EOUST Organizational Chart | EOUST Field Structure Map

Federal Bureau of Investigation (FBI)

FBI Organizational Chart | FBI Field Structure Map

Federal Bureau of Prisons (BOP)

BOP Organizational Chart | Federal Prison Industries | National Institute of Corrections | BOP Field Structure Map

[Foreign Claims Settlement Commission \(FCSC\)](#)

[FCSC Organizational Chart](#)

[INTERPOL Washington - United States National Central Bureau \(INTERPOL\)](#)

[INTERPOL Washington Organizational Chart](#)

[Justice Management Division \(JMD\)](#)

[JMD Organizational Chart](#)

[National Security Division \(NSD\)](#)

[NSD Organizational Chart](#)

[Office for Access to Justice \(ATJ\)](#)

[ATJ Organizational Chart](#)

[Office of Community Oriented Policing Services \(COPS\)](#)

[COPS Organizational Chart](#)

[Office of Information Policy \(OIP\)](#)

[OIP Organizational Chart](#)

[Office of Justice Programs \(OJP\)](#)

[OJP Organizational Chart](#)

[Office of Legal Counsel \(OLC\)](#)

[OLC Organizational Chart](#)

[Office of Legal Policy \(OLP\)](#)

[OLP Organizational Chart](#)

[Office of Legislative Affairs \(OLA\)](#)

[OLA Organizational Chart](#)

[Office of Professional Responsibility \(OPR\)](#)

[OPR Organizational Chart](#)

[Office of Public Affairs \(PAO\)](#)

[PAO Organizational Chart](#)

[Office of Tribal Justice \(OTJ\)](#)

[OTJ Organizational Chart](#)

[Office of the Inspector General \(OIG\)](#)

[OIG Organizational Chart](#)

[Office of the Pardon Attorney \(OPA\)](#)

[OPA Organizational Chart](#)

[Office on Violence Against Women \(OVW\)](#)

[OVW Organizational Chart](#)

[Professional Responsibility Advisory Office \(PRAO\)](#)

[PRAO Organizational Chart](#)

[Tax Division \(TAX\)](#)

[TAX Organizational Chart](#)

[United States Marshals Service \(USMS\)](#)

[USMS Organizational Chart](#) | [USMS Field Structure Map](#)

United States Parole Commission (USPC)

USPC Organizational Chart

Former Organization, Mission and Functions Manuals can be found in the Department of Justice Archive.

Manual Last Updated: June 2012

Updated August 1, 2017

Exhibit 29

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Sizing Up the Executive Branch Fiscal Year 2016



Sizing Up the Executive Branch

Fiscal Year 2016

*This document provides a brief summary of the size
of the Executive Branch of the Federal Government.*

U.S. Office of Personnel Management
Planning and Policy Analysis
Data Analysis Group

Contents

Purpose	3
Coverage	3
Types of Employment	3
Size of the Executive branch of the Federal Government	4
Figure 1. Federal Executive Branch Employment by Fiscal Year	4
Table 1. Federal Executive Branch Employment by Fiscal Year	4
Figure 2. Federal Executive Branch Employment for the Past Year by Month	5
Table 2. Federal Executive Branch Employment for the Past Year by Month	5
Table 3. NSFTP Federal Executive Branch Employment by Cabinet level Agency	6
Table 4. Comparing the Federal Executive Branch Workforce to U.S. Population	7
Additional Details.....	7

Purpose

This document presents an overview of the size of the Executive Branch of the Federal Government, providing the public and analysts access to commonly requested information about the size of the Federal Civilian Workforce.

This document presents data in the form of tables and graphs on the current and historical size of the Executive Branch of the Federal Government.

Coverage

The Office of Personnel Management (OPM) data coverage is often equated to the Federal Executive civilian workforce. The data excludes a few major components of the Executive Branch (most notably the Postal Service and intelligence agencies) and includes some parts or components of the Legislative and Judiciary Branch. OPM data excludes contractors and contract employees.

For specific exclusions and inclusions, visit FedData on the OPM's website: <https://www.opm.gov/policy-data-oversight/data-analysis-documentation/federal-employment-reports/#url=SDM> .

Types of Employment

Each Federal employee has a particular work schedule, type of appointment, tenure, and appointment authority, among other variables, which dictate the "type" of his or her employment.¹ This paper examines two types of employment: (1) Non-Seasonal Full-Time Permanent (NSFTP) Employees² [about 89% of the workforce] and (2) all other employees [about 10% of the workforce].³

¹ There are six types of employment but data are always filtered to employees in pay status, meaning only employees currently receiving a paycheck are included.

² This category includes all employees working a 40-hour work week year round with no absolute end date.

³ Other category comprises the other five employment types. This category includes part time, seasonal, and non-permanent employees.

Size of the Executive branch of the Federal Government

This section presents basic data, in the form of tables and graphs, on the current and historical size of Executive Branch of the Federal Government.

Figure 1. Federal Executive Branch Employment by Fiscal Year

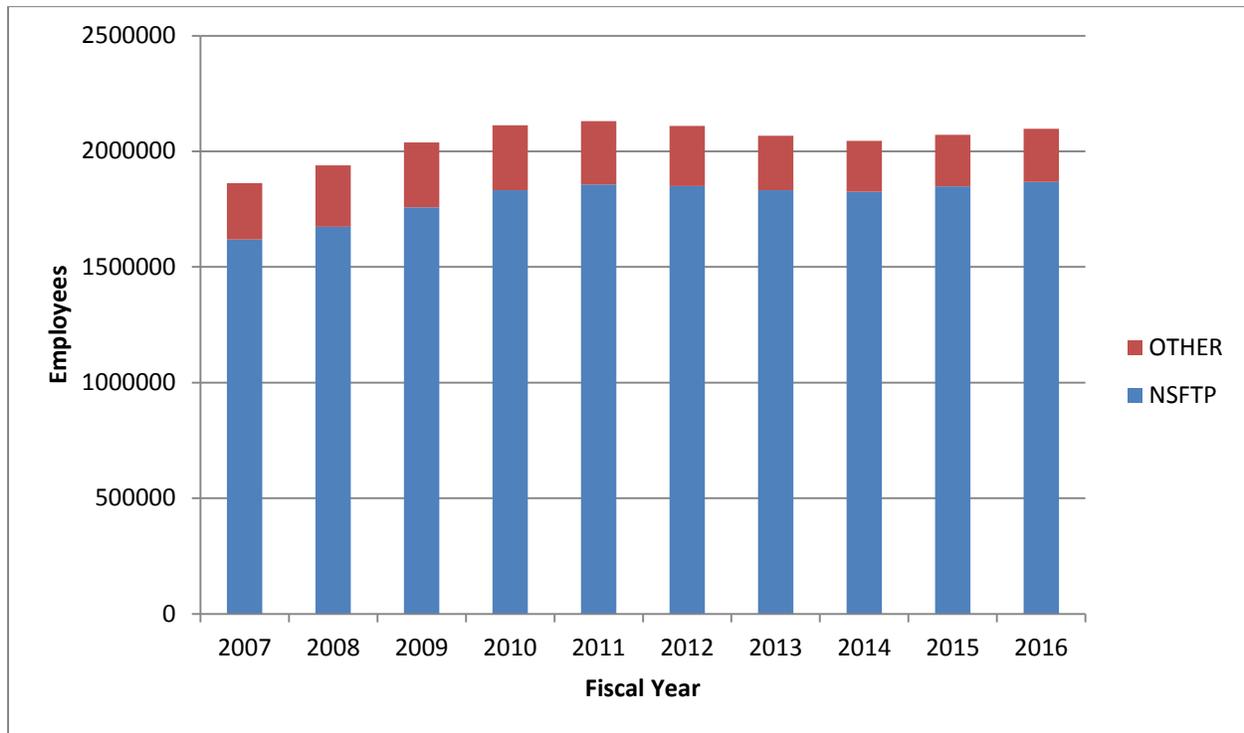


Figure 1 shows the size of the Executive Branch of the Federal workforce over the last ten fiscal years. NSFTP employees in 2016 make up 89.08% of the employees in the Executive Branch of the Federal workforce.

Table 1. Federal Executive Branch Employment by Fiscal Year

YEAR	NSFTP	NSFTP % CHANGE	OTHER	OTHER % CHANGE	TOTAL	TOTAL % CHANGE
2007	1,618,159	-	244,245	-	1,862,404	-
2008	1,673,249	3.40%	265,572	8.73%	1,938,821	4.10%
2009	1,757,105	5.01%	281,078	5.84%	2,038,183	5.12%
2010	1,831,719	4.25%	281,491	0.15%	2,113,210	3.68%
2011	1,856,580	1.36%	273,709	-2.76%	2,130,289	0.81%
2012	1,850,311	-0.34%	259,910	-5.04%	2,110,221	-0.94%
2013	1,831,723	-1.00%	235,539	-9.38%	2,067,262	-2.04%
2014	1,825,762	-0.33%	219,945	-6.62%	2,045,707	-1.04%
2015	1,848,494	1.25%	223,222	1.49%	2,071,716	1.27%
2016	1,868,027	1.06%	229,011	2.59%	2,097,038	1.22%

Table 1 shows the size of the Executive Branch of the Federal workforce over the last ten fiscal years and is the data used to create Figure 1 above. The table also shows the percentage change from year to year.

Figure 2. Federal Executive Branch Employment for the Past Year by Month

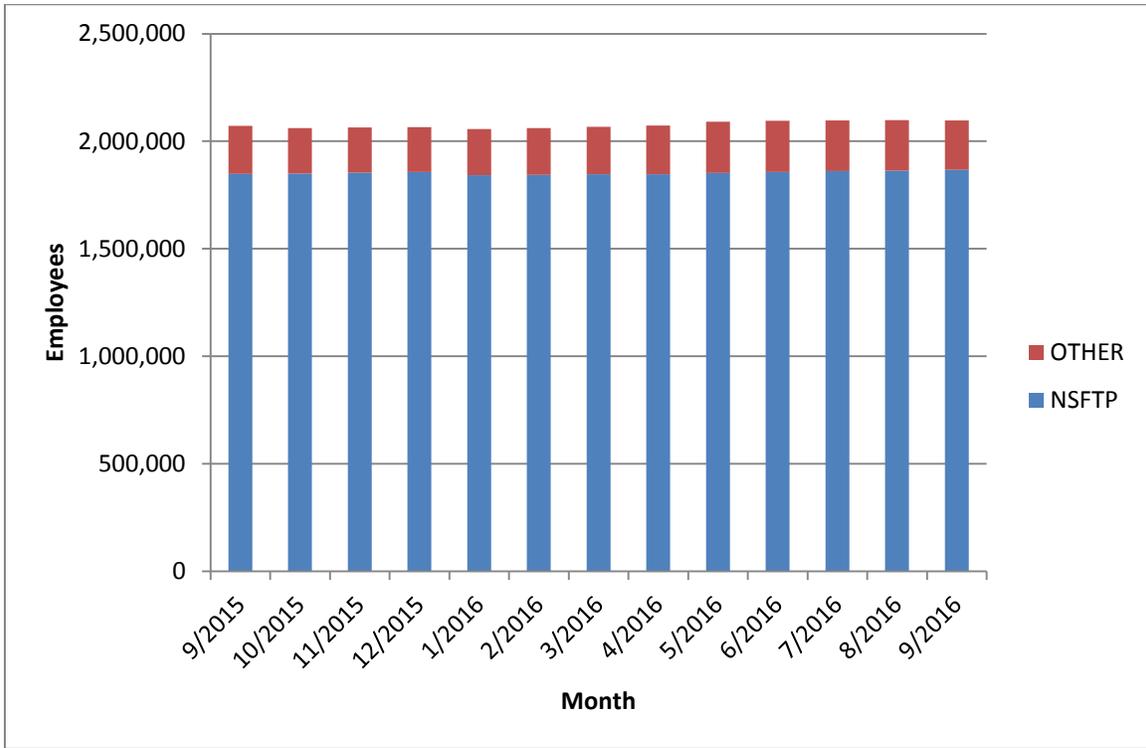


Figure 2 shows the size of the Executive Branch of the Federal workforce over the last thirteen months.

Table 2. Federal Executive Branch Employment for the Past Year by Month

DATE	NSFTP	OTHER	TOTAL
9/2015	1,848,494	223,222	2,071,716
10/2015	1,849,888	211,416	2,061,304
11/2015	1,854,504	209,239	2,063,743
12/2015	1,856,870	208,996	2,065,866
1/2016	1,842,075	214,610	2,056,685
2/2016	1,844,405	216,844	2,061,249
3/2016	1,847,116	220,527	2,067,643
4/2016	1,847,053	225,595	2,072,648
5/2016	1,853,314	237,284	2,090,598
6/2016	1,857,544	237,574	2,095,118
7/2016	1,861,002	235,666	2,096,668
8/2016	1,863,720	235,141	2,098,861
9/2016	1,868,027	229,011	2,097,038

Table 2 shows the size of the Executive Branch of the Federal workforce over the last thirteen months and is the data used to create Figure 2 above.

Table 3. NSFTP Federal Executive Branch Employment by Cabinet level Agency

AGENCY	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015	FY2016
DEPARTMENT OF EDUCATION	3,789	3,825	3,769	4,010	4,066	3,899	3,865	3,815	3,862	3,973
DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT	9,237	9,445	9,147	9,397	9,269	8,982	8,547	8,255	8,059	7,883
DEPARTMENT OF STATE	8,009	8,428	8,622	8,959	9,443	9,761	10,142	10,068	10,121	10,500
DEPARTMENT OF ENERGY	14,286	14,803	15,134	15,757	15,548	15,041	14,739	14,341	14,443	14,499
DEPARTMENT OF LABOR	14,406	14,322	14,762	15,387	15,190	15,705	15,354	15,077	15,086	14,996
DEPARTMENT OF COMMERCE	32,177	32,924	33,642	33,711	34,501	35,013	34,550	34,857	35,249	35,661
DEPARTMENT OF THE INTERIOR	51,953	51,828	52,796	53,460	53,393	53,156	50,959	49,082	48,798	49,679
DEPARTMENT OF TRANSPORTATION	52,530	53,549	55,433	56,151	56,092	55,614	54,374	53,684	53,822	53,992
DEPARTMENT OF HEALTH AND HUMAN SERVICES	52,842	53,325	56,124	58,946	60,303	61,168	62,086	62,099	63,324	65,431
DEPARTMENT OF AGRICULTURE	78,993	78,369	78,962	80,510	79,899	76,785	74,117	72,889	73,663	74,465
DEPARTMENT OF DEFENSE	70,111	72,133	76,622	81,179	85,818	86,135	85,579	89,547	89,521	86,662
DEPARTMENT OF THE TREASURY	94,603	93,961	98,361	99,868	96,232	92,397	89,852	86,049	84,050	82,556
DEPARTMENT OF JUSTICE	102,716	104,282	108,349	112,688	112,867	113,358	112,342	110,427	111,010	112,900
DEPARTMENT OF THE AIR FORCE	145,987	142,957	148,133	158,039	166,338	161,574	159,499	156,195	156,594	158,270
DEPARTMENT OF HOMELAND SECURITY	134,850	147,533	157,573	161,273	166,210	169,116	168,348	167,422	166,777	169,547
DEPARTMENT OF THE NAVY	166,714	172,392	180,913	189,389	191,975	192,500	188,599	187,723	195,815	201,543
DEPARTMENT OF THE ARMY	216,076	225,881	241,329	257,947	255,487	251,257	241,609	235,951	233,035	230,765
DEPARTMENT OF VETERANS AFFAIRS	215,336	236,761	255,012	268,187	277,461	285,436	297,528	308,176	324,639	333,264
ALL OTHER AGENCIES	153,544	156,531	162,422	166,861	166,488	163,414	159,634	160,105	160,626	161,441
ALL	1,618,159	1,673,249	1,757,105	1,831,719	1,856,580	1,850,311	1,831,723	1,825,762	1,848,494	1,868,027

Table 3 shows the NSFTP size of Federal Executive Branch employment by cabinet level agencies over the last ten fiscal years. The Department of Defense, Department of Homeland Security, Department of Justice, Department of the Air Force, Department of the Army, Department of the Navy, Department of Health and Human Services, and the Department of Veterans Affairs has grown the most over the past ten fiscal years. Over the last ten fiscal years those eight agencies have grown by nearly 250,000 employees.

Table 4. Comparing the Federal Executive Branch Workforce to U.S. Population

POPULATION	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
TOTAL U.S. POPULATION*	301,231,207	304,093,966	306,771,529	309,348,193	311,663,358	313,998,379	316,204,908	318,563,456	320,896,618	323,127,513
NSFTP FEDERAL EMPLOYEES	1,618,159	1,673,249	1,757,105	1,831,719	1,856,580	1,850,311	1,831,723	1,825,762	1,848,494	1,868,027
NSFTP FEDERAL EMPLOYEES PER 1,000 AMERICANS	5.372	5.502	5.728	5.921	5.957	5.893	5.793	5.731	5.760	5.781

Table 4 compares the size of the Executive Branch of the Federal workforce to the United States population over the past ten years. The U.S. population data comes from the Census Bureau website⁴ (the source of some information in Table 4 above) at <http://www.census.gov/>. It is important to note that this table considers the entire U.S. population, not simply the labor force or workforce. Census data is in no way linked to OPM data.

Additional Details

For any data requests, the OPM produces an online data tool, FedScope, which is updated quarterly: <http://www.fedscope.opm.gov/>. Many of the tables and figures above can be replicated in FedScope, with the option for much more detail. The tool is best utilized via Internet Explorer. For all other inquiries, contact the Data Analysis Group through FedStats at FedStats@opm.gov.

⁴ The U.S. population estimates came from the Census Bureau's July release:

<https://www.census.gov/data/tables/time-series/demo/popest/intercensal-2000-2010-national.html> and

<https://www.census.gov/data/tables/2016/demo/popest/nation-total.html>



U.S. Office of Personnel Management

Planning and Policy Analysis

1900 E Street, NW, Washington, DC 20415

OPM.GOV