



PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD
WASHINGTON, D.C. 20511

October 16, 2018

Charlie Savage
The New York Times
1627 I Street NW
7th Floor
Washington, DC 20006
savage@nytimes.com

Re: PCLOB FOIA 2017-021

Dear Mr. Savage:

I am writing in response to your request for records under the Freedom of Information Act ("FOIA") received on May 31, 2017 seeking the disclosure of the Privacy and Civil Liberties Oversight Board's ("PCLOB") report on the implementation of Presidential Policy Directive 28: Signals Intelligence Activities ("PPD-28").

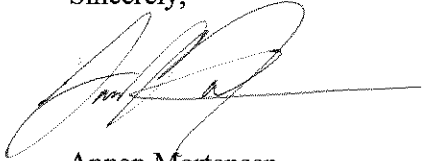
A search was conducted and a document was located that is responsive to your request. However, release of the document required consultation with other executive branch agencies. The appropriate executive branch agencies have reviewed the document and provided the PCLOB with any relevant FOIA exemptions that should be applied prior to disclosure. This letter includes a redacted version of the PPD-28 report.

After consulting with the appropriate executive branch agencies, redactions pursuant to Exemptions 1, 3, 5, and 6 of the FOIA, 5 U.S.C. § 552 (b)(1), (b)(3), (b)(5), and (b)(6), are applied. Exemption 1 protects from disclosure information that has been deemed classified "under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy." Exemption 3 incorporates certain nondisclosure provisions contained in other federal statutes into the FOIA. Exemption 5 protects certain inter- and intra-agency memorandums or letters protected by the deliberative process privilege, and Exemption 6 protects information the disclosure of which would "constitute a clearly unwarranted invasion of personal privacy." Redactions have been clearly marked with the corresponding exemption.

You may contact me or the PCLOB's FOIA Public Liaison Eric Broxmeyer at (202) 296-4617 or foia@pclob.gov for further assistance and to discuss any aspect of your request. Additionally, you may contact the Office of Government Information Services ("OGIS") at the National Archives and Records Administration ("NARA") to inquire about the FOIA mediation services they offer. The contact information for OGIS is Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001; email at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

If you are not satisfied with my response to this request, you may administratively appeal by writing to the PCLOB Freedom of Information Act Appeal Authority, at 800 N. Capitol St., NW, Washington, DC 20002, or you may submit an appeal via email to foia@pclob.gov. Your appeal must be postmarked or electronically transmitted within ninety calendar days from the date of this letter.

Sincerely,

A handwritten signature in black ink, appearing to read 'Annan Mortensen', with a long horizontal flourish extending to the right.

Annan Mortensen
Acting Freedom of Information Act Officer
Attorney-Advisor
(202) 296-2706

Mason Clutter

From: Savage, Charlie <savage@nytimes.com>
Sent: Wednesday, May 31, 2017 4:31 PM
To: Sharon Bradford Franklin; Mason Clutter; dni-foia@dni.gov
Cc: David McCraw; Ian MacDougal
Subject: NYT FOIA request for two PCLOB documents

Dear PCLOB and Office of the Director of National Intelligence,

Under the Freedom of Information Act, I request access to (and declassification review of, if necessary) the following documents:

- the PPD-28 report PCLOB transmitted to Congress about five months ago
- the current version of PCLOB's draft report on Executive Order 12333 issues

As a member of the news media engaged in gathering information about government activities for public education, I request a fee waiver, please.

I am located at
c/o The New York Times
1627 I Street NW
7th Floor
Washington, DC 20006

Thank you for assistance with this matter.

Charlie Savage
The New York Times

Phone: 202-862-0317
Cell: 202-369-6653



PRIVACY & CIVIL LIBERTIES OVERSIGHT BOARD

(U) Report to the President on the Implementation of Presidential Policy Directive 28: Signals Intelligence Activities

TABLE OF CONTENTS

(U) Part I Introduction..... 1

(U) Part II Significant Changes in Practice due to the Issuance of PPD-28..... 5

(U) Part III Analysis and Recommendations..... 12

(U) Part IV Conclusion..... 18

(U) Annexes:

(U) A. Separate Statement by Board Members Rachel Brand and Elisebeth Collins..... 20

(U) B. Separate Statement by Board Members James Dempsey and Patricia Wald..... 23

I. (U) Introduction

(U) On January 17, 2014, President Obama signed Presidential Policy Directive – 28, *Signals Intelligence Activities* (“PPD-28”), which provides principles to guide “why, whether, when, and how the United States conducts signals intelligence activities[.]”¹ The directive recognizes both that “[t]he collection of signals intelligence is necessary for the United States to advance its national security and foreign policy interests and to protect its citizens

¹ (U) See Presidential Policy Directive – 28, *Signals Intelligence Activities* (January 17, 2014) (*hereinafter* “PPD-28”), available at <https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>.

Classified By (b) (6) Attorney-Advisor, PCLOB
~~Derived From: Multiple Sources~~
~~Declassify On: 20411231~~

and the citizens of its allies and partners from harm” and that “all persons have legitimate privacy interests in the handling of their personal information.”² In an effort to protect the national security of the United States while respecting privacy and civil liberties, the directive codifies current practices and establishes new principles related to the collection, use, retention, dissemination, and oversight of signals intelligence, particularly with regard to personal information of non-U.S. Persons.

(U) The directive is divided into six sections. Section 1 outlines the following principles: (a) signals intelligence shall be authorized by and undertaken only in accordance with the law; (b) privacy and civil liberties shall be integral in the planning of signals intelligence activities; (c) the collection of foreign private commercial information or trade secrets is authorized only to protect national security; and (d) signals intelligence activities shall be as tailored as feasible. Section 2 limits the use of bulk signals intelligence to six permissible purposes. Section 3 and the classified annex refine the processes for establishing signals intelligence priorities and requirements, and reviewing sensitive targets. Section 4 requires the development and implementation of policies that provide certain safeguards to information regarding all persons, regardless of their nationality or where they reside, when it is collected through signals intelligence activities. Section 5 requests, and in most instances requires, that reports on specific aspects of the implementation of the directive be written and provided to the White House. Section 6 provides a general description of how the directive interacts with other legal authorities.

(U) The Privacy and Civil Liberties Oversight Board (“PCLOB”) is issuing this report in response to Section 5 of PPD-28, which encourages the PCLOB to provide the White House with a report that assesses the implementation of any matters contained within PPD-28 that fall within the Board’s mandate.³ This report represents the PCLOB’s assessment of PPD-28 matters that fall within the Board’s mandate to “. . . continually review the regulations, policies, and procedures, and the *implementation* of the regulations, policies, and procedures, of the departments, agencies, and elements of the executive branch relating to efforts to protect the Nation from terrorism to ensure that privacy and civil liberties are protected.”⁴ On December 14, 2016, the Board voted unanimously to adopt this report. Board Members Brand and Collins wrote a joint separate statement, which is appended to this report in Annex A. Board Members Dempsey and Wald wrote a joint separate statement, which is appended to this report in Annex B.

² (U) PPD-28 at p.1.

³ (U) PPD-28 § 5(b).

⁴ (U) 42 U.S.C. § 2000ee(d)(2)(A)(emphasis added).

(U) The PCLOB's review of the implementation of PPD-28 is based on classified briefings and discussions with IC elements.⁵ The review also included examination of the IC element and IC-wide policies that implement PPD-28. In addition, the PCLOB reviewed public comments, primarily from non-governmental organizations ("NGOs"), regarding PPD-28.

(U) Shortly after the President issued PPD-28, the Office of the Director of National Intelligence ("ODNI") created an intra-IC working group to come up with a common approach to implement the requirements of PPD-28 and to determine what, if any, additional protections are warranted beyond what PPD-28 requires.⁶ In July 2014, the ODNI released a status report on the development and implementation of procedures pursuant to PPD-28.⁷ The status report describes the ODNI's evaluation of possible additional dissemination and retention safeguards for personal information and includes key principles that the IC elements must follow as they adopt policies and procedures under PPD-28.⁸ In January and February 2015, the IC elements issued public procedures regarding the implementation of PPD-28.⁹ In February 2015 and January 2016, the ODNI released reports that summarize the impact and results of the IC's signals intelligence reform activities.¹⁰ The ODNI reports also inform this report.

(U) The ways in which the IC elements have implemented the directive to date have varied based on their missions and authorities, access to signals intelligence information, and information systems. While PPD-28 applies to every element of the IC, the directive has the greatest impact on the IC elements that (1) collect signals intelligence or information

⁵ (U) The following IC elements were consulted: the Office of the Director of National Intelligence ("ODNI"); National Security Agency ("NSA"); Central Intelligence Agency ("CIA"); Federal Bureau of Investigation ("FBI"); Department of State, Bureau of Intelligence and Research ("State INR"); Drug Enforcement Administration, Office of National Security Intelligence ("DEA ONSI"); Department of Treasury, Office of Intelligence and Analysis ("Treasury OIA"); Department of Homeland Security, Office of Intelligence and Analysis ("DHS I&A"); Department of Homeland Security, U.S. Coast Guard ("DHS USCG"); Department of Energy, Office of Intelligence and Counterintelligence ("DOE/IN"); National Reconnaissance Office ("NRO"); National Geospatial Agency ("NGA"); Defense Intelligence Agency ("DIA"); U.S. Air Force; and other government personnel that support these IC elements.

⁶ (U) Office of the Director of National Intelligence, Safeguarding the Personal Information of All People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28 (July 2014) (hereinafter "ODNI Status Report"), p. 1, *available at* https://www.dni.gov/files/documents/1017/PPD-28_Status_Report_Oct_2014.pdf.

⁷ (U) ODNI Status Report.

⁸ (U) ODNI Status Report at pp.1-2.

⁹ (U) U.S. Intelligence Community Policies & Procedures to Safeguard Personal Information Collected through SIGINT, *available at* <https://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties> (mid-way through the page).

¹⁰ (U) Office of the Director of National Intelligence, Signals Intelligence Reform 2015 Anniversary Report (February 3, 2015), *available at* <https://icontherecord.tumblr.com/ppd-28/2015>. Office of the Director of National Intelligence, 2016 Progress Report on Changes to Signals Intelligence Activities (January 22, 2016), *available at* <https://icontherecord.tumblr.com/ppd-28/2016>.

that they consider to be covered by PPD-28 and (2) possess and handle unevaluated signals intelligence. This includes portions of the Department of Defense (“DoD”), Central Intelligence Agency (“CIA”), and, to a lesser extent, the Federal Bureau of Investigation (“FBI”). The portions of the DoD that either collect signals intelligence, possess and handle unevaluated signals intelligence, or both under Executive Order 12333 do so under the direction, authority delegation or control of the Director of the National Security Agency (“NSA”).

~~(S//NF)~~ As a result, this report focuses on NSA, CIA, and to a lesser degree, the FBI. We note that signals intelligence has traditionally been an NSA function. FBI states in its PPD-28 procedures that it does not conduct signals intelligence activities.¹¹ However, FBI interprets footnote 6 of PPD-28 to mean that PPD-28 applies to FBI in some way, so it is applying PPD-28 to communications collected under Section 702 of the Foreign Intelligence Surveillance Act (“FISA”), a non-signals intelligence activity.¹² Similarly, CIA notes in its PPD-28 procedures that it applies PPD-28 to both signals intelligence activities and some non-signals intelligence activities.¹³ The CIA’s guiding principle is that PPD-28 is intended to apply to

(b) (1) (A), (b) (3) (A)
(b) (1) (A), (b) (3) (A) Accordingly, as a matter of internal policy, the CIA has determined that it will apply PPD-28 to

(b) (1) (A), (b) (3) (A)
(b) (1) (A), (b) (3) (A) NSA, CIA, and FBI have decided to apply PPD-28 to communications collected under FISA Section 702.

(U) This report is limited to an examination of how different IC elements have implemented PPD-28; it takes no position on the policy enumerated in PPD-28. The report discusses NSA, CIA and FBI’s implementation of PPD-28. It does not focus on the other IC elements because they are primarily consumers of intelligence derived from signals intelligence after it has been evaluated and disseminated by NSA in accordance with the NSA’s PPD-28 procedures.

(U) The report consists of four parts. Part II follows this introduction and describes changes in practices resulting from the implementation of PPD-28. Part III analyzes the IC’s implementation of PPD-28 and provides four recommendations. Part IV provides conclusions. Following the conclusions, the report includes two separate statements.

11 (U) FBI PPD-28 public procedures § I.
12 (U) FBI staff Briefing to PCLOB staff on PPD-28 (December 15, 2015).
13 (U) Internal CIA policy, Activities to Which the CIA Will Apply PPD-28 § I(A).
14 (U) Internal CIA policy, Activities to Which the CIA Will Apply PPD-28 § I(B).
15 (U) Internal CIA policy, Activities to Which the CIA Will Apply PPD-28 § I(B).

II. (U) Significant Changes in Practice due to the Issuance of PPD-28

a. (U) Collection

(U) The National Intelligence Priorities Framework (“NIPF”) is the primary mechanism to create, remove, communicate, and manage national intelligence priorities that guide IC collection and analytic activities.¹⁶ The National Signals Intelligence Committee (“SIGCOM”) reviews signals intelligence collection requests to ensure that they are consistent with the NIPF, and validates priorities for NSA’s signals intelligence collection.¹⁷ PPD-28 Section 3 and the classified annex to PPD-28 supplement the signals intelligence priorities review and approval process. Section 3 requires departments and agencies to identify signals intelligence priorities and requirements so that the heads of those departments and agencies can annually review and determine whether those identified priorities and requirements should be maintained. In making the determination, the value of the signals intelligence activities must be considered in light of the risks entailed in conducting these activities. Risks include “risks created by the constantly evolving technological and geopolitical environment,” “inherent concerns raised when signals intelligence can be collected only in bulk,” and “the risk of damage to our national security interests and our law enforcement, intelligence-sharing, and diplomatic relationships should our capabilities or activities be compromised.”¹⁸

(b) (1) (A), (b) (3) (A)



¹⁶ (U) Intelligence Community Directive (“ICD”) 204: National Intelligence Priorities Framework, § D1 (January 2 2015).

¹⁷ (U) Letter from the ODNI GC to Justin S. Antonipillai (Counselor, Department of Commerce) and Ted Dean (Deputy Assistant Secretary, International Trade Administration), p. 5 (February 22, 2016).

¹⁸ (U) PPD-28 § 3.

¹⁹ (U) PPD-28 Classified Annex § 2.

²⁰ (U) PPD-28 Classified Annex § 2.

²¹ (U) PPD-28 Classified Annex § 4.

²² (U) NSA staff briefing to PCLOB staff on PPD-28 (December 16, 2015); CIA staff briefing to PCLOB staff on PPD-28 (December 17, 2016).



b. (U) Use

(U) Section 2 of PPD-28 requires the IC to use signals intelligence collected in bulk only for the purposes of detecting and countering six threats: (1) espionage and threats and activities directed by foreign powers; (2) threats to the U.S. and its interests from terrorism; (3) threats to the U.S. and its interests from weapons of mass destruction; (4) cybersecurity threats; (5) threats to the U.S., allied Armed Forces or U.S./allied personnel; and (6) transnational criminal threats.²⁵ In its status report, ODNI directed that “in the case of unevaluated SIGINT information contained in datasets or repositories, Intelligence Community element policies should reinforce existing analytic practices and standards whereby analysts must seek to structure queries or other search terms and techniques to identify intelligence information relevant to a valid intelligence or law enforcement task; focus queries about persons on the categories of intelligence information responsive to an intelligence or law enforcement requirement; and minimize the review of personal information not pertinent to intelligence or law enforcement requirements.”²⁶

(U) Prior to the issuance of PPD-28, as a practical matter NSA’s use of signals intelligence collected in bulk was already limited to the six abovementioned purposes.²⁷ However, these limitations were not codified in NSA procedure until the directive was issued.²⁸ As a result of PPD-28, NSA has memorialized the fact that it limits its use of signals intelligence collected in bulk to the six permissible purposes listed in PPD-28.²⁹

~~(S//NF)~~ NSA’s general querying³⁰ standards have not changed as a result of PPD-28. However, as a result of PPD-28, NSA has memorialized the fact that queries must be

²³ (U) ODNI staff briefing to PCLOB staff on PPD-28 (January 21, 2016).

²⁴ (U) ODNI staff briefing to PCLOB staff on PPD-28 (January 21, 2016).

²⁵ (U) PPD-28 § 2.

²⁶ (U) ODNI Status Report at p. 5.

²⁷ (U) NSA staff briefing to PCLOB staff on PPD-28 (December 16, 2015).

²⁸ (U) NSA staff briefing to PCLOB staff on PPD-28 (December 16, 2015).

²⁹ (U) NSA public procedures §5.2.

³⁰ (U) NSA’s PPD-28 procedures and E.O. 12333 procedures use the phrase “selection term” to refer to the process of using individual terms to “effect or defeat selection of particular communications for the

designed to return foreign intelligence and, if a query is intended to run against a database containing unminimized signals intelligence collected in bulk, the query may be run only to address one of the six authorized purposes for bulk SIGINT collection.³¹ Prior to PPD-28, NSA's procedures focused on protecting U.S. person information ("USPI") rather than personal information of all individuals regardless of nationality.³² However, NSA reports that even prior to the issuance of PPD-28, it would run queries – whether designed to return USPI, non-USPI, or both – only to obtain information related to specific foreign intelligence targets or topics.³³

~~(S//NF)~~ Limiting the use of signals intelligence collected in bulk to the purposes that are listed in the directive (b) (1) (A), (b) (3) (A)

(b) (1) (A), (b) (3) (A)

However, in the past, CIA would also

use this data to (b) (1) (A), (b) (3) (A)

(b) (1) (A), (b) (3) (A)

As a result of PPD-28, CIA is only permitted to query signals intelligence collected in bulk to the six purposes that are listed in the directive and has memorialized this requirement.³⁷

~~(S//NF)~~ Like NSA, prior to PPD-28, CIA's querying rules focused on protecting U.S. person information ("USPI") (b) (1) (A), (b) (3) (A)

(b) (1) (A), (b) (3) (A)

As a result of PPD-28, CIA has

decided to require its analysts to "structure query terms and techniques in a manner reasonably designed to identify intelligence relevant to an authorized intelligence requirement and minimize the review of personal information not relevant to an authorized intelligence requirement."³⁹

(U) FBI's public PPD-28 procedures state that "[t]he FBI will focus queries about persons, regardless of nationality, on the categories of intelligence information responsive

purpose of interception." Classified Annex to DoD Manual 5240.01 §2. NSA applies the restrictions on the use of "selection terms" to queries of repositories containing signals intelligence information. For purposes of consistency, we use the term "query" to refer to NSA's searches of its signals intelligence repositories.

³¹ (U) NSA staff briefing to PCLOB staff on PPD-28 (December 16, 2015). See also NSA PPD-28 public procedures §5.2.

³² (U) NSA staff briefing to PCLOB staff on PPD-28 (December 16, 2015).

³³ (U) NSA staff briefing to PCLOB staff on PPD-28 (December 16, 2015).

³⁴ (U) CIA staff briefing to PCLOB staff on PPD-28 (December 17, 2015).

³⁵ (U) CIA staff briefing to PCLOB staff on PPD-28 (December 17, 2015).

³⁶ (U) CIA staff briefing to PCLOB staff on PPD-28 (December 17, 2015).

³⁷ (U) CIA public PPD-28 procedures p.3.

³⁸ (U) CIA staff call with PCLOB on follow-up questions (August 4, 2016).

³⁹ (U) CIA public PPD-28 procedures p.5.

to an intelligence requirement or an authorized law enforcement activity.”⁴⁰ Under FISA Section 702, the Bureau was already required to structure query terms to identify information relevant to a valid intelligence requirement or an authorized law enforcement activity.⁴¹

c. (U) Retention

(U) PPD-28 establishes three requirements concerning the retention of non-U.S. person information: (1) personal information of non-U.S. persons shall be retained only if comparable information of U.S. persons may be retained pursuant to Section 2.3 of E.O. 12333; (2) personal information of non-U.S. persons shall be subject to the same retention period as comparable information concerning U.S. persons; and (3) personal information that has not been determined to fit within an E.O. 12333 Section 2.3 category (also referred to as unevaluated information) shall be retained for no longer than five years unless the DNI expressly determines that continued retention is in the interest of national security.⁴² These are not absolute requirements; they are to be applied equally to the personal information of all persons, regardless of nationality, *to the maximum extent feasible consistent with the national security.*⁴³

(U) With respect to the first provision, NSA, CIA, and FBI procedures repeat PPD-28’s requirement that personal information of non-U.S. persons shall only be retained if comparable information of U.S. persons may be retained pursuant to section 2.3 of E.O. 12333.⁴⁴ Similarly, these IC elements’ procedures bring into effect the second requirement to harmonize the retention periods for USPI and non-USPI.⁴⁵ With respect to the third requirement, the ODNI issued Intelligence Community Directive (“ICD”) 107-01, a policy governing requests for extensions beyond the five-year retention period.⁴⁶ The policy requires the submission of written requests that (1) are approved by high-level officials, (2) are as narrowly tailored as possible, and (3) include a mission need for the information and the views on the adequacy of the proposed protections from the senior official responsible for matters involving the protections of privacy and civil liberties.⁴⁷ NSA complied with the ODNI mandate in ICS 107-01 to inventory its data by the end of 2015 to

⁴⁰ (U) FBI public PPD-28 procedures § III(A)(1)(c).

⁴¹ (U) FBI staff briefing to PCLOB staff on PPD-28 (December 15, 2015). FBI PPD-28 Fact Sheet p.2.

⁴² (U) PPD-28 § 4(a)(i).

⁴³ (U) PPD-28 § 4(a), emphasis added.

⁴⁴ (U) NSA PPD-28 public procedures do not recite this statement, but they state that the “NSA’s Supplemental Procedures extend comparable safeguards currently provided for U.S. Persons to all persons, regardless of nationality.” p.1; CIA PPD-28 public procedures p.4; FBI PPD-28 public procedures § III(1)(b).

⁴⁵ (U) NSA Public Procedures § 6.1(a); CIA Public Procedures p.4; FBI Public Procedures § III(1)(b).

⁴⁶ (U) Intelligence Community Standard (“ICS”) 107-01: Continued Retention of SIGINT Under PPD-28 (February 2, 2015).

⁴⁷ (U) ICS 107-01: Continued Retention of SIGINT Under PPD-28 §§ D(1)-(2).

(b) (3) (A), (b) (5)

determine which data sets, if any, might require such extension requests.

(b) (3) (A), (b) (5)

~~(S//NF)~~ At NSA, the five-year temporary retention period does not represent a change in practice. According to NSA, as a general matter, even prior to PPD-28, NSA retained unevaluated signals intelligence information, for no more than five years, regardless of the nationality of the persons to whom the information pertained, since NSA could not rule out the possibility that unevaluated signals intelligence information of or concerning non-U.S. persons might also include USPI.⁵⁰ By contrast, the requirement to seek DNI approval for an extension led NSA to change its practices. Prior to PPD-28's issuance, requests for extension were approved within NSA.⁵¹ CIA explained that

(b) (1) (A), (b) (3) (A)

(b) (1) (A), (b) (3) (A)

(b) (1) (A), (b) (3) (A)

As noted above, FBI elected to apply the relevant provisions of PPD-28 to information collected pursuant to FISA Section 702.⁵³ This includes the five-year retention period. FBI indicated that the five-year retention period is not a change in practice for FISA Section 702 data because the FBI's FISA Section 702 minimization procedures already impose a five-year retention limit for information that has never been reviewed.⁵⁴

d. (U) Dissemination

~~(U//FOUO)~~ PPD-28 states that personal information of non-U.S. persons shall be disseminated only if comparable USPI may be disseminated under E.O. 12333 Section 2.3, to the maximum extent feasible consistent with the national security.⁵⁵ ODNI has interpreted this to mean that IC elements may disseminate the personal information of non-U.S. persons only if the personal information relates to an authorized foreign

⁴⁸ (U) ODNI staff briefing to PCLOB staff re. PPD-28 (January 21, 2016).

⁴⁹ (U) ODNI staff briefing to PCLOB staff re. PPD-28 (January 21, 2016).

⁵⁰ (U) NSA staff briefing to PCLOB staff on PPD-28 (December 16, 2015).

⁵¹ (U) NSA staff briefing to PCLOB staff on PPD-28 (December 16, 2015).

⁵² (U) CIA staff briefing to PCLOB staff on PPD-28 (December 17, 2015).

⁵³ (U) FBI PPD-28 public procedures § I.

⁵⁴ ~~(S//NF)~~ FBI staff Briefing to PCLOB staff on PPD-28 (December 15, 2015). FBI 702 Minimization Procedures § III.G.1.a. (Jul. 15, 2015) ("FISA-acquired information that has been retained but never reviewed shall be destroyed five years from the expiration date of the certification authorizing the collection.").

⁵⁵ (U) PPD-28 §4(a)(i).

intelligence requirement.⁵⁶ The mere fact that signals intelligence is about a non-U.S. person is not, absent additional information, sufficient to disseminate such information.

~~(S//NF)~~ NSA reports that its implementation of this requirement has not resulted in substantial changes in practice with regards to its disseminated SIGINT products. NSA's past practice was to limit all signals intelligence activities, including the dissemination of personal information of non-U.S. persons in disseminated SIGINT products, to those necessary to accomplish its foreign intelligence mission.⁵⁷ Nevertheless, the NSA has modified its training and guidance to include the requirement that it disseminate personal information of non-U.S. persons in disseminated SIGINT products only if related to an authorized foreign intelligence requirement.⁵⁸

(b) (3) (A), (b) (5)

~~(U//FOUO)~~ NSA's PPD-28 procedures state that the NSA may include non-USPI in reporting if it is "related to an authorized foreign intelligence requirement."⁶⁰ This standard differs from the standard that governs dissemination of USPI: USPI may be disseminated if doing so is "necessary to understand the foreign intelligence information or assess its importance."⁶¹ Section 4 of PPD-28 states that IC element PPD-28 policies and procedures, including provisions that govern dissemination, are to be applied equally to the personal information of all persons, regardless of nationality, but only "to the maximum extent feasible consistent with the national security."⁶²

(b) (3) (A), (b) (5)

~~(S//NF)~~ CIA has a pre-existing requirement that personal information relating to non-U.S. persons could be disseminated only if it related to a foreign intelligence purpose.⁶³ CIA has determined that PPD-28 required no change in existing practice. However, it incorporated this requirement into its public procedures, which now specify that if the CIA is "disseminating personal information concerning a foreign person because it is foreign

⁵⁶ (U) ODNI Status Report at p. 5.

⁵⁷ (U) NSA staff briefing to PCLOB staff on PPD-28 (December 16, 2015). *See, for example*, NSA Public Procedures § 7.

⁵⁸ (U) NSA staff briefing to PCLOB staff on PPD-28 (December 16, 2015).

⁵⁹ (U) NSA staff briefing to PCLOB staff on PPD-28 (December 16, 2015).

⁶⁰ (U) NSA staff briefing to PCLOB staff on PPD-28 follow-up questions (August 4, 2016); NSA PPD-28 public procedures (emphasis added).

⁶¹ (U) NSA staff briefing to PCLOB staff on PPD-28 follow-up questions (August 4, 2016); USSID 18 § 7.2.c (emphasis added).

⁶² (U) NSA staff briefing to PCLOB staff on PPD-28 (December 16, 2015).

⁶³ (U) CIA staff briefing to PCLOB staff on PPD-28 (December 17, 2015).

intelligence, the information must be *related to* an authorized intelligence requirement, [and] cannot be disseminated solely because of the person's foreign status."⁶⁴ This standard differs from the standard that governs the dissemination of USPI derived from electronic surveillance: "Information about a United States person derived from electronic surveillance may be retained and disseminated . . . if the identity of the U.S. person and all personally identifiable information are deleted. . . . If the information cannot be sanitized in such a fashion because the identity is *necessary or reasonably believed that it may become necessary*, to understand or assess the information, that identity may be retained or disseminated outside the CIA along with the information if . . ." the information fits within a list of categories that are similar to those found in E.O. 12333 Section 2.3.⁶⁵ As noted above, pursuant to PPD-28 Section 4, dissemination provisions are to be applied equally to the personal information of all persons, regardless of nationality, to the maximum extent feasible consistent with the national security. ~~(b) (1) (A), (b) (3) (A)~~

~~(b) (1) (A), (b) (3) (A)~~

(U) FBI stated that it already meets the dissemination requirements of PPD-28. Even prior to the Directive, all FBI targets under Section 702 of FISA were connected with a full investigation.⁶⁷ Accordingly, FBI contends that all personal information of non-U.S. persons was obtained in the course of a lawful foreign intelligence, counterintelligence, or international terrorism investigation and therefore may be disseminated under PPD-28 and the ODNI guidance.⁶⁸

⁶⁴ (U) CIA public PPD-28 procedures p.5 (emphasis added).

⁶⁵ ~~(S//NF)~~ Internal Agency Policy, Law and Policy Governing the Conduct of Intelligence, Appendix D(1) (emphasis added).

⁶⁶ (U) CIA staff briefing to PCLOB staff on PPD-28 (December 17, 2015).

⁶⁷ ~~(U//FOUO)~~ See FBI Domestic Investigations and Operations Guide (DIOG) §§ 7.9 and 18.7.3 (Released October 15, 2011, Updated November 19, 2012).

⁶⁸ (U) FBI PPD-28 Fact Sheet p.2.

III. (U) Analysis and Recommendations

a. (U) Clarifying the Scope of PPD-28

~~(U//FOUO)~~ The President issued PPD-28 to establish special requirements and procedures for the conduct of signals intelligence activities. PPD-28 does not define “signals intelligence activities.”⁶⁹ Nor did the ODNI. It was left to each IC element to determine how to apply PPD-28 to its respective activities.

~~(S//NF)~~ As a result, the application varies across the IC. ~~(b) (1) (A), (b) (3) (A)~~

~~(b) (1) (A), (b) (3) (A)~~



⁶⁹ (U) Footnote 3 of PPD-28 clarifies that “[u]nless otherwise specified, this directive shall apply to signals intelligence activities conducted in order to collect communications . . .”

⁷⁰ (U) Internal CIA Policy, Activities to Which the CIA Will Apply PPD-28 § I(B).

~~(S//NF)~~ (b) (1) (A), (b) (3) (A) FBI applies PPD-28 to communications collected under Section 702 of FISA, but exempts communications collected under FISA Title I or Sections 704 and 705(b) of FISA.⁷¹ FBI's rationale is that PPD-28 should not apply to the latter FISA activities because those surveillances require an individualized finding of probable cause. Furthermore, some IC elements, such as the (b) (1) (A), (b) (3) (A)

(b) (1) (A), (b) (3) (A)

~~(U//FOUO)~~ It is not unusual for individual IC elements to apply different procedures to similar types of data. This is often a function of the authorities and missions unique to each IC element. However, the lack of a common understanding as to the activities to which PPD-28 applies has led to inconsistent interpretation and could lead to compliance traps, especially as IC elements engage in information sharing.

(U) Recommendation 1: The Board recommends that the National Security Council ("NSC") and ODNI issue criteria for determining which activities or types of data will be subject to PPD-28's requirements. The ODNI could establish these criteria by issuing a list of PPD-28 activities or by promulgating guidelines for applying PPD-28. This guidance may be classified, in whole or in part, in order to provide the appropriate level of detail.

⁷¹ (U) FBI public PPD-28 procedures § I.

⁷² (U) Email from ODNI Deputy General Counsel Bradley Brooker to PCLOB Attorney Advisor (b) (6)

(b) (6) dated September 14, 2016.

Whatever the format, the ODNI guidance should be in writing and applied uniformly throughout the IC.

b. (U) Application of PPD-28 to Multi-Sourced Systems

i. (U) Background

(U) The IC conducts both targeted and bulk collection of intelligence information through a variety of sources that include signals intelligence. In some cases, IC elements have created databases and tools that store and use signals intelligence collected in bulk together with signals intelligence collected in a targeted manner or store signals intelligence together with information collected through a different intelligence discipline (i.e. human source intelligence). We refer to the mixing of multiple sources of intelligence sources as “multi-sourced” systems.

(U) PPD-28 requires the IC to provide specific protections to personal information derived from signals intelligence and limits the ways in which the IC may use signals intelligence collected in bulk. As outlined above, it establishes three requirements (with the qualifier “to the maximum extent feasible with the national security”) for the retention of personal information collected through signals intelligence activities: (1) personal information of non-U.S. persons shall only be retained if comparable information of U.S. persons may be retained pursuant to Section 2.3 of E.O. 12333; (2) personal information of non-U.S. persons shall be subject to the same retention period as that of U.S. persons; and (3) personal information of all individuals, regardless of nationality, that has not been determined to fit within an E.O. 12333 Section 2.3 category shall be retained for no longer than five years unless the DNI expressly determines that continued retention is in the interest of national security.⁷³

(U) In addition, PPD-28 specifies that signals intelligence collected in bulk may only be used for detecting and countering: (1) espionage and threats and activities directed by foreign powers; (2) threats to the U.S. and its interests from terrorism; (3) threats to the U.S. and its interests from weapons of mass destruction; (4) cybersecurity threats; (5) threats to the U.S., allied Armed Forces or U.S./allied personnel; and (6) transnational criminal threats.⁷⁴

(U) These requirements do not apply to intelligence collected through other disciplines.

⁷³ (U) PPD-28 § 4(a)(i).

⁷⁴ (U) PPD-28 § 2.

ii. (U) Application of PPD-28 to Multi-Sourced Systems at CIA

~~(S//NF)~~ CIA primarily collects intelligence through human sources, also known as human intelligence or HUMINT. (b) (1) (A), (b) (3) (A)

(b) (1) (A), (b) (3) (A)
(b) (1) (A), (b) (3) (A)

As noted above, we refer to these as “multi-sourced systems” since they contain information collected through more than one intelligence discipline.

~~(S//NF)~~ (b) (1) (A), (b) (3) (A)

(b) (1) (A), (b) (3) (A)

(b) (1) (A), (b) (3) (A) Now, CIA has imposed a requirement that limits its use of signals intelligence collected in bulk to the permissible uses that are listed in PPD-28.⁷⁶

~~(S//NF)~~ In addition, pursuant to PPD-28, CIA will retain personal information derived from signals intelligence that has not been determined to fit within an E.O. 12333 Section 2.3 category for no more than five years unless the DNI approves continued retention.⁷⁷ In general, CIA’s existing systems for storing data (b) (1) (A), (b) (3) (A)

(b) (1) (A), (b) (3) (A)

To comply with PPD-28, CIA is undertaking a long-term, substantial effort to identify signals intelligence in its holdings

(b) (1) (A), (b) (3) (A)

(b) (1) (A), (b) (3) (A) CIA has explained that it is using a phased approach to identify SIGINT in its holdings, (b) (1) (A), (b) (3) (A)

(b) (1) (A), (b) (3) (A) One such database is (b) (3) (A) The vast majority of data in (b) (3) (A) consists of (b) (1) (A), (b) (3) (A) which CIA is treating as signals intelligence covered by PPD-28. Some of the remaining data in (b) (3) (A) such as (b) (1) (A), (b) (3) (A), (b) (3) (A) does not fit within the list of activities to which CIA applies PPD-28.⁸¹

⁷⁵ (U) CIA staff briefing to PCLOB staff on PPD-28 (December 17, 2015).
⁷⁶ (U) CIA staff briefing to PCLOB staff on PPD-28 (December 17, 2015).
⁷⁷ (U) CIA public PPD-28 procedures p.5.
⁷⁸ (U) CIA staff call with PCLOB staff on PPD-28 follow-up questions (August 10, 2016).
⁷⁹ (U) CIA staff call with PCLOB staff on PPD-28 follow-up questions (August 10, 2016).
⁸⁰ (U) CIA staff call with PCLOB staff on PPD-28 follow-up questions (August 10, 2016).
⁸¹ (U) Internal CIA Policy, Activities to Which the CIA Will Apply PPD-28 § I(A); CIA staff call with PCLOB staff on PPD-28 follow-up questions (November 30, 2016).

(b) (1) (A), (b) (3) (A)

~~(S//NF)~~ In order to ensure that all information subject to PPD-28 receives PPD-28 protections, the CIA has, at times, opted to apply PPD-28 protections to all information within multi-sourced systems even if the CIA assesses that PPD-28 does not apply to all data within the systems. For example, the CIA is applying PPD-28 rules to all information within (b) (1) (A), (b) (3) (A)

(b) (1) (A), (b) (3) (A)

The Board appreciates CIA's efforts to comply with the directive and recognizes that it may be both more protective of civil liberties and more economical from a technical, training and resource perspective to be over-inclusive in applying PPD-28 provisions. (b) (1) (A), (b) (3) (A)

(b) (1) (A), (b) (3) (A)

As the CIA continues to

review its holdings for signals intelligence (b) (1) (A), (b) (3) (A)

(b) (1) (A), (b) (3) (A)

the Board expects that the CIA will seek out solutions that comply with

PPD-28's requirements (b) (1) (A), (b) (3) (A)

(U) Recommendation 2: IC elements should consider both the mission and privacy implications of applying PPD-28 to multi-sourced systems.

c. (U) Potential Impacts of Increased Sharing of Raw Signals Intelligence

(U) IC elements' authorities and access to information may change over time. When such changes occur, the IC will need to ensure that it remains in compliance with PPD-28. For example, the IC is working to issue new procedures pursuant to the unenumerated paragraph of E.O. 12333 Section 2.3. That provision requires IC elements to establish written procedures approved by the Attorney General in order to engage in the sharing of unevaluated signals intelligence.⁸⁵ Unevaluated information is information that has neither

⁸² (U) CIA staff call with PCLOB staff on PPD-28 follow-up questions (November 30, 2016).

⁸³ (U) CIA staff call with PCLOB staff on PPD-28 follow-up questions (November 30, 2016).

⁸⁴ (b) (1) (A), (b) (3) (A)

⁸⁵ (U) E.O. 12333 permits IC elements to disseminate information "to each appropriate element within the Intelligence Community for purposes of allowing the recipient element to determine whether the information is relevant to its responsibilities and can be retained by it, except that information derived from signals intelligence may only be disseminated or made available to Intelligence Community elements in accordance with procedures established by the Director in coordination with the Secretary of Defense and approved by the Attorney General."

been evaluated for relevance to foreign intelligence purposes nor minimized to restrict personal information not relevant to understanding the intelligence value of the data.

(U) If approved by the Attorney General, procedures governing the sharing of unevaluated signals intelligence (“2.3 Procedures”) would allow NSA to share unevaluated, unminimized signals intelligence information with IC elements that do not currently have access to such information. IC elements that request and are granted access to unevaluated signals intelligence will be able to assess the information under their own authorities and in support of their specific mission requirements. This would cause a significant change for these IC elements, and one that would affect the application of PPD-28 to these elements. Therefore, prior to obtaining this information, IC elements would need to review and likely update PPD-28 procedures, guidance, and trainings. In particular, any IC elements that receive unevaluated signals intelligence would likely need to update their retention and dissemination practices governed by PPD-28 Section 4(a).

~~(S//NF)~~ We understand that the 2.3 Procedures, if approved, will permit IC elements to request access to raw SIGINT from NSA. NSA may choose to make raw SIGINT available (i) through NSA’s systems; (ii) through a shared IC or other Government capability, such as a cloud-based environment [e.g., the Intelligence Community Information Technology Enterprise (“IC ITE”)]; or (iii) by transferring some or all of the information to the recipient IC element’s information systems. Only information that can be afforded appropriate handling, storage, retention, and access protections by the recipient IC element will be made available.⁸⁶ NSA is responsible for ensuring compliance with PPD-28 retention requirements for its own data stored in IC ITE. By contrast, IC elements that receive data from the NSA and retain it in their own systems bear the responsibility of retaining unevaluated signals intelligence in compliance with PPD-28.

~~(S//SI//NF)~~ As discussed above, to comply with PPD-28, IC elements must age off unevaluated signals intelligence within five years unless the DNI grants an extension.⁸⁷ Recipient IC elements may need to update information technology systems that handle data tagging and age-off to comply with this requirement. They may also need to provide additional training or guidance to personnel who will be handling unevaluated signals intelligence for the first time.

(U) IC elements obtaining first-time access to unevaluated signals intelligence pursuant to 2.3 procedures should consider how PPD-28 impacts their retention, use, and dissemination practices. IC elements receiving formally disseminated signals intelligence

⁸⁶ ~~(U//FOUO)~~ IC ITE is a common, cloud architecture intended to enable greater integration, information sharing and safeguarding across the IC.

⁸⁷ ~~(S//SI//NF)~~ By contrast, if the NSA shared unevaluated signals intelligence available to other IC elements through IC ITE and also retains control over the data, NSA would bear the responsibility for applying the appropriate retention period to the raw data.

may rely on the disseminating IC element's determination that the personal information is foreign intelligence and that it is relevant to the authorized purpose of the dissemination. IC elements gaining access to unevaluated signals intelligence should assume the responsibility of determining whether personal information meets the PPD-28 use, retention, and dissemination rules.

(U) Recommendation 3: The Board recommends that the NSC and ODNI ensure that any IC elements obtaining first-time access to unevaluated signals intelligence update their PPD-28 use, retention and dissemination practices, procedures, and trainings before receiving any unevaluated data.

(U) In part, the purpose of PPD-28 is to build trust, both domestically and internationally, in the IC's process for conducting signals intelligence activities. One aspect of building trust is transparency. In January and February 2015, IC elements issued public procedures regarding the implementation of PPD-28.⁸⁸ Since IC element authorities or access to information may change over time, it is important that each IC element (1) periodically review its PPD-28 procedures to ensure that the procedures continue to reflect current practices, (2) periodically review its PPD-28 practices to ensure that they remain consistent with the directive and ODNI guidance, and (3) update its publicly available procedures, consistent with classification requirements, to reflect changes in practice. This will be particularly the case if and when the NSA's 2.3 Procedures are approved and issued.

(U) Recommendation 4: The Board recommends that to the extent consistent with the protection of classified information, IC elements promptly update their public PPD-28 procedures to reflect any pertinent future changes in practices and policy, including those changes due to issuance of new procedures under Section 2.3 of E.O. 12333.

IV. (U) Conclusion

~~(U//FOUO)~~ The President encouraged the Board to provide a report that assesses the implementation of any matters concerned in the Directive that fall within the Board's mandate.⁸⁹ PPD-28 is still new and the IC still faces many questions of first impression in interpreting its requirements. As implementation takes shape, the ODNI may consider monitoring PPD-28 questions, compliance issues, and incidents with the aim of identifying any systemic problems or IC best practices.

⁸⁸ (U) U.S. Intelligence Community Policies & Procedures to Safeguard Personal Information Collected through SIGINT, *available at* <https://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties> (mid-way through the page).

⁸⁹ (U) PPD-28 § 5(b).

~~(U//FOUO)~~ PPD-28 requires that privacy and civil liberties be integral considerations in the planning of U.S. signals intelligence activities.⁹⁰ NSA's public procedures assign the Director of the Civil Liberties and Privacy Office with the responsibility to provide advice on PPD-28 implementation, and to review privacy and civil liberties safeguards for new or unique SIGINT collection programs. The Board understands that the NSA has formalized its assessment of civil liberties and privacy into its reviews of operational activities. CIA's public PPD-28 procedures similarly require consultation with the CIA's Privacy and Civil Liberties Officer when executing novel or unique collection activities, or when considering significant changes to current collection activities. Other IC elements may also consider creating internal processes, patterned after those at NSA and CIA, to ensure that privacy and civil liberty interests are accounted for throughout the intelligence process. We also invite further dialogue between the IC and the Board as PPD-28 implementation progresses.

⁹⁰ (U) PPD-28 § 1(b).

ANNEX A

(U) Separate Statement of Board Members Rachel Brand and Elisebeth Collins

(U) We write separately to express our concern with certain aspects of the implementation of PPD-28. The Board's review of PPD-28 did not extend to evaluating the PPD's underlying policy decision to equalize treatment of non-U.S. Persons and U.S. Persons in the field of foreign intelligence gathering. While we have significant reservations about the wisdom of this policy judgment, particularly when the intelligence services of other nations do not afford Americans the same courtesy (and have not been inspired to do so by PPD-28), we leave that policy question to the side in this statement.

(U) During our interactions with IC elements in the course of the Board's review, we observed a great deal of confusion among the agencies as to whether and how each should apply PPD-28. We do not believe the Administration provided adequate guidance to individual agencies on which programs should fall within the scope of the Directive. Perhaps the primary cause of the agencies' implementation challenges was the decision to base the entire PPD-28 framework on the term "signals intelligence," which has no definition in PPD-28. It has long been understood in the IC to refer to certain NSA activities; one senior IC official described it to us as referring to "what the NSA does when the NSA does it." Basing the PPD's parameters on this undefined term, particularly when many agencies covered by PPD-28 did not have what they previously considered to be a "signals intelligence" function, left agencies scrambling to figure out whether and how to apply PPD-28 to their operations. The briefings we received on PPD-28's implementation left us with the impression that the agencies understood ODNI's guidance to mean that each of them should find *something* to which they could apply the PPD, which they then did, even at the cost of over application.

(U) We have significant concerns that agencies may apply PPD-28's retention requirements beyond the letter or even the spirit of the PPD due to a combination of policy judgments and technical challenges.

~~(S//NF)~~ The CIA, for example, has decided to apply PPD-28 to a broad range of activities, including some that it explicitly acknowledges "are not SIGINT."⁹¹ The CIA has also decided to apply PPD-28 to entire datasets that contain *any* records it has deemed covered by PPD-28 (b) (1) (A), (b) (3) (A)

(b) (1) (A), (b) (3) (A)

For example, during the Board's review, we were informed that the CIA was applying PPD-28 to (b) (3) (A). The Board recently provided its final report to the IC for accuracy review. In our separate statement, we expressed serious reservations (b) (3) (A)

(b) (3) (A)

for the reasons set forth below. At that point, the IC provided us with the "clarification" (b) (3) (A), (b) (5)

⁹¹ (U) Internal CIA Policy, Activities to Which the CIA Will Apply PPD-28, sec. I.A.

⁹² (U) See PCLOB Report on PPD-28 at pp. 15-16.

(b) (3) (A), (b) (5) [REDACTED] We welcome this clarification, although it reinforces our perception of a somewhat chaotic implementation process. Moreover, we are surprised that such a consequential decision (b) (1) (A) [REDACTED] (b) (3) (A) [REDACTED] has not yet been made.

(S//NF) We urge the CIA *not* to apply PPD-28's retention rules to (b) (3) (A) [REDACTED] unless and until it develops a way to avoid over-application of the Directive. (b) (3) (A) [REDACTED] contains (b) (1) (A), (b) (3) (A) [REDACTED] records collected by a variety of means, including some that are clearly not "signals intelligence." It contains (b) (1) (A), (b) (3) (A) [REDACTED] (b) (1) (A), (b) (3) (A) [REDACTED]

If PPD-28's (b) (1) (A), (b) (3) (A) [REDACTED] retention rules are applied wholesale to this system, (b) (1) (A), (b) (3) (A) [REDACTED] records (b) (1) (A), (b) (3) (A) [REDACTED] (b) (1) (A), (b) (3) (A) [REDACTED] that were *never intended to be covered by PPD-28*, will be deleted two years from now. Although the CIA does not regularly maintain qualitative metrics as to the value of older records, in 2015 the CIA determined that (b) (1) (A), (b) (3) (A) [REDACTED] queries returned data more than five years old. Therefore, it is reasonable to assume that if the CIA applies PPD-28's retention rules (b) (1) (A), (b) (3) (A) [REDACTED] queries will return more limited information.

(U) We also have concerns about the FBI's implementation of PPD-28. As noted above, agencies were left with a sense that they must "do something" to comply with PPD-28, leading to a mismatch between even the spirit of PPD-28 and its application. In the course of our review, the FBI informed us that although it does not engage in "signals intelligence," it felt compelled to apply PPD-28's *retention* restrictions to some FBI activity because the FBI is mentioned in a footnote in the PPD's *collection* section.⁹³ Based on this extrapolation from a footnote, the FBI applies PPD-28 to FISA section 702. Even if it makes sense to apply PPD-28's target nomination and review process⁹⁴ to collection under Section 702, it does not follow that the PPD's retention requirements should be applied to Section 702, a program consisting of targeted collection that is already subject to court authorization and extensive minimization procedures.

(S//NF) Finally, PPD-28 has been applied inconsistently among agencies even as to the same activity. (b) (1) (A), (b) (3) (A) [REDACTED] the FBI applies PPD-28 to FISA Section 702 but not to FISA Sections 704 or 705(b), or FISA Title I,⁹⁵ (b) (1) (A), (b) (3) (A) [REDACTED] (b) (1) (A), (b) (3) (A) [REDACTED] By contrast, the NSA applies PPD-28 to all of the above. (b) (1) (A), (b) (3) (A) [REDACTED]

(b) (1) (A), (b) (3) (A) [REDACTED] (b) (1) (A), (b) (3) (A) [REDACTED]. This disparity among applications creates increased

⁹³ (U) PPD-28, sec. 3, note 6. Section 3 of PPD-28 directs senior policymakers to consider the "special concerns" associated with certain potential collection activities. Footnote 6 excludes from this Section certain FBI activities. From this exclusion from the PPD's *collection* section, the FBI concluded that it should apply the PPD's *retention* provisions to at least some FBI activity.

⁹⁴ (S//NF) See PPD-28, sec. 3, and Annex, secs. 2-7.

⁹⁵ (U) FBI, Presidential Policy Directive 28 Policies and Procedures (Feb. 2, 2015), sec. I, *passim*.

⁹⁶ (U) Internal CIA Policy, Activities to Which the CIA Will Apply PPD-28, secs. I.B & C.

risk of compliance problems and of future over-application of the PPD (b) (1) (A), (b) (3) (A)
(b) (1) (A), (b) (3) (A) The agencies apparently were left to make these decisions without clear guidance from senior policymakers.

(U) We urge senior policymakers to carefully consider the impact of application of PPD-28 and to suspend application of the retention requirements at the CIA and any other IC elements that currently lack the technical means to avoid over-application of the PPD.

ANNEX B

(U) Separate Statement of Board Members James Dempsey and Patricia Wald

(U) We write separately to register our additional views on Presidential Policy Directive 28 (“PPD-28”). We address three issues related to the implementation of the directive by the Intelligence Community (“IC”): (1) the importance to U.S. global leadership of the policy expressed in PPD-28; (2) the IC’s decisions about the term “signals intelligence activities” and the scope of PPD-28; and (3) the implementation of PPD-28 with respect to mixed data sets or “multi-sourced systems,” as defined in the Board’s report.⁹⁷

(U) Policy expressed in PPD-28

(U) Although the Board’s report “takes no position on the policy enumerated in PPD-28,” we write in support of the directive.

(U) PPD-28 was a milestone. It responded to an important and difficult issue in U.S. foreign intelligence practice: How to conduct necessarily robust collection of communications data outside the United States while respecting the privacy rights of non-U.S. persons — privacy rights inherent, according to the long-standing policy of the United States, in all human beings. This challenge has become magnified in the Internet age. Electronic communications offer a rich source of valuable intelligence. The use of global communications networks has become woven into the daily business and personal lives of literally billions of people. Demonstrated respect for the privacy rights of the non-U.S. person communicating electronically on global networks is vital to ensuring a strong leadership role for the United States.

(U) By codifying for the first time significant limits on intelligence activities affecting non-U.S. persons outside the United States, the directive gave substance to our government’s claim to respect the human rights of all individuals. It affirmed and strengthened the role of the United States as the world’s leader by (1) establishing express limits on intelligence activities, even as it reaffirmed the need for robust intelligence capabilities; (2) promoting transparency about those limits; and (3) establishing a greater degree of equivalence, where feasible, between protections for the personal information of U.S. persons and non-U.S. persons.

(U) But PPD-28 is necessary not solely because of human rights. The protections in PPD-28 are also intended to strengthen U.S. relationships with foreign allies, to protect U.S.

⁹⁷ (U) See PCLOB Report on PPD-28 at p. 14.

commercial, financial, and economic interests, and to minimize risks to intelligence sources and methods.⁹⁸

(U) The protections of PPD-28 played a key role in the restoration of a legal framework allowing U.S. companies to collect and process data about Europeans. That legal framework, the EU-U.S. Privacy Shield, is crucial to the Internet services that create jobs in the United States. A move away from the protections in PPD-28 would jeopardize trans-Atlantic data flows, to the peril of U.S. commercial interests.

(U) “Signals intelligence activities” and Intelligence Community interpretation

(U) Turning to implementation, it is important to echo the note in the Board’s report that PPD-28’s protections are not absolute but rather are expressly intended to be applied in a manner that does not jeopardize national security.⁹⁹ PPD-28 applies to, but does not define, “signals intelligence activities.” In the absence of a definition, it was left to the IC to determine which activities would be subject to PPD-28’s requirements.

(U) In our view, IC elements went about identifying the activities subject to PPD-28 with appropriately careful consideration of the purpose and intent of PPD-28 and what the directive calls the “evolving technological and geopolitical environment” in which our intelligence agencies operate.¹⁰⁰

~~(S//NF)~~ One central feature of this environment is the (b) (1) (A)
(b) (1) (A) in the past, (b) (1) (A)
(b) (1) (A) However, in today’s digital world (b) (1) (A)
(b) (1) (A) Nevertheless, the privacy interests of individuals and the harms that could occur if the fact of collection were disclosed are the same.

⁹⁸ (U) PPD-28 at p.1 (“At the same time, signals intelligence activities and the possibility that such activities may be improperly disclosed to the public pose multiple risks. These include risks to: our relationships with other nations, including the cooperation we received from other nations on law enforcement, counterterrorism, and other issues; our commercial, economic, and financial interests, including a potential loss of international trust in U.S. firms and the decreased willingness of other nations to participate in international data sharing, privacy, and regulatory regimes; the credibility of our commitment to an open, interoperable, and secure global Internet; and the protection of intelligence sources and methods.”)

⁹⁹ (U) Section 4’s safeguards are to be implemented “[t]o the maximum extent feasible consistent with the national security.” PPD-28 at p. 8.

¹⁰⁰ (U) PPD-28 at pp. 3, 6.

~~(S//NF)~~ To interpret PPD-28 narrowly, (b) (1) (A), (b) (3) (A)
(b) (1) (A), (b) (3) (A) would have failed to address the risks presented by other activities yielding communications data, such as (b) (1) (A), (b) (3) (A)
(b) (1) (A), (b) (3) (A)

(U) In our view, the ODNI appropriately chose an implementation approach that is consistent with the intent of the directive and the challenges to which it responded.¹⁰¹ We commend ODNI's approach. The U.S. Government should not provide public assurances that it is collecting and processing foreign communications under rules designed to protect privacy and civil liberties while quietly exempting certain activities yielding the same types of information. Otherwise, when the inconsistency was exposed, it would damage the credibility of the United States.

(U) While we understand and applaud the IC-wide intent to avoid overly formalistic applications of PPD-28, the Board's report registers concerns raised by divergent applications of PPD-28 across the IC. The current, fragmented approach may cause confusion and could prove inadequate to address the risks of improper disclosure identified in the directive. Efforts to implement the Board's first recommendation — that the NSC and the ODNI "issue criteria for determining which activities or types of data will be subject to be PPD-28's requirements" — should follow the ODNI's guidance to avoid an "overly narrow" application of PPD-28's protections.

(U) CIA's application of PPD-28 to multi-sourced systems

~~(S//NF)~~ Keeping in mind the importance of PPD-28 in strengthening the United States' position as a global leader and recognizing the value of applying PPD-28 consistently across the same types of data when collected by different means, it is possible to turn to more granular questions of implementation. When it comes to the application of PPD-28 to specific datasets (b) (3) (A) based on the assessments developed by the IC so far, we do not believe that the Board is in a position to definitively assess the operational impact.

(b) (1) (A), (b) (3) (A)

~~(S//NF)~~ While application of PPD-28's five-year rule will result in the aging off of (b) (1) (A), (b) (3) (A) data that is returned by queries, the CIA has presented us with no information about (b) (1) (A), (b) (3) (A) how its loss would impact (b) (1) (A), (b) (3) (A)

¹⁰¹ (U) See ODNI Status Report at p. 2 n. 1 ("Intelligence Community elements should not take an overly narrow approach to defining what information will be protected under their PPD-28 procedures.").

¹⁰² (U) Email from CIA Privacy and Civil Liberties Officer Benjamin Huebner to PCLoB Board Member Elisebeth Collins (December 7, 2016).

(b) (1) (A), (b) (3) (A)

This lack of a meaningful assessment of efficacy is part of a broader interest that the Board has highlighted since its earliest work. We recognize that value is a matter of judgment, and we appreciate that no one is likely to say that a dataset or an item of information would never be useful. However, PPD-28 and much other intelligence policy is based on a balancing of concerns. In this case, as in so many other cases, the relevance and efficacy components of the equation are unmeasured (at least the Board has been presented with no measurements). In the absence of specific information about relevance and efficacy, we believe it is appropriate to note only that this issue merits continued attention.

(b) (1) (A), (b) (3) (A)

(b) (1) (A), (b) (3) (A)

To question that decision would require an assessment of relevance and efficacy that has not been made available to us.

(b) (1) (A), (b) (3) (A)

(b) (1) (A), (b) (3) (A)

~~(S//NF)~~ We understand that the CIA has undertaken a long-term effort to identify its data holdings (b) (1) (A), (b) (3) (A). This is an important initiative with potentially positive consequences for data management, operational efficiency, and privacy that go beyond the CIA's implementation of PPD-28.

(U) LIST OF SOURCES

- (U) Presidential Policy Directive – 28, Signals Intelligence Activities (January 17, 2014), available at <https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>.
- (U) 42 U.S.C. § 2000ee.
- (U) Office of the Director of National Intelligence, Safeguarding the Personal Information of All People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28 (July 2014), available at https://www.dni.gov/files/documents/1017/PPD_28_Status_Report_Oct_2014.pdf.
- (U) Office of the Director of National Intelligence, Signals Intelligence Reform 2015 Anniversary Report (February 3, 2015), available at https://icontherecord.tumblr.com/ppd_28/2015.
- (U) Office of the Director of National Intelligence, 2016 Progress Report on Changes to Signals Intelligence Activities (January 22, 2016), available at https://icontherecord.tumblr.com/ppd_28/2016.
- (U) FBI Presidential Policy Directive 28: Policy and Procedures (“FBI PPD-28 public procedures”) (Feb. 2, 2015).
- (U) FBI staff Briefing to PCLOB staff on PPD 28 (December 15, 2015).
- (U) Internal CIA policy, Activities to Which the CIA Will Apply PPD 28.
- (U) Intelligence Community Directive (“ICD”) 204: National Intelligence Priorities Framework (January 2 2015).
- (U) Letter from the ODNI GC to Justin S. Antonipillai (Counselor, Department of Commerce) and Ted Dean (Deputy Assistant Secretary, International Trade Administration) (February 22, 2016).
- (U) NSA staff briefing to PCLOB staff on PPD 28 (December 16, 2015).
- (U) CIA staff briefing to PCLOB staff on PPD 28 (December 17, 2016).
- (U) ODNI staff briefing to PCLOB staff on PPD 28 (January 21, 2016).
- (U) USSID SP0018: Supplemental Procedures for the Collection, Processing, Retention, and Dissemination of Signals Intelligence Information and Data Containing Personal Information of Non-United States Persons (“NSA public procedures”) (January 12, 2015).
- (U) Classified Annex to DoD Manual 5240.01.
- (U) CIA staff call with PCLOB on follow-up questions (August 4, 2016).
- (U) CIA Signals Intelligence Activities Public Policy.
- (U) Intelligence Community Standard (“ICS”) 107-01: Continued Retention of SIGINT Under PPD-28 (February 2, 2015).
- (U) FBI 702 Minimization Procedures (Jul. 15, 2015).
- (U) NSA staff briefing to PCLOB staff on PPD 28 follow-up questions (August 4, 2016)

- (U) FBI Domestic Investigations and Operations Guide (DIOG) (Released October 15, 2011, Updated November 19, 2012).
- (U) Presidential Policy Directive 28 Application to the FBI: Fact Sheet.
- (U) Email from ODNI Deputy General Counsel Bradley Brooker to PCLOB Attorney Advisor Renee Gewercman, dated September 14, 2016.
- (U) CIA staff call with PCLOB staff on PPD 28 follow-up questions (August 10, 2016).
- (U) CIA staff call with PCLOB staff on PPD 28 follow-up questions (November 30, 2016).
- (U) E.O. 12333: United States Intelligence Activities (2008).
- (U) Office of the Director of National Intelligence Presidential Policy Directive 28 Policies and Procedures, available at <https://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties> (mid-way through the page).
- (U) Department of Treasury, PPD-28 Procedures for the Office of Intelligence and Analysis, available at <https://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties> (mid-way through the page).
- (U) Department of Homeland Security, Office of Intelligence and Analysis, Safeguarding Personal Information Collected from Signals Intelligence Activities, available at <https://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties> (mid-way through the page).
- (U) U.S. Department of State, Bureau of Intelligence and Research, Presidential Policy Directive 28- Policies and Procedures, available at <https://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties> (mid-way through the page).
- (U) Drug Enforcement Administration, Office of National Security Intelligence, Presidential Policy Directive 28- Policies and Procedures, available at <https://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties> (mid-way through the page).
- (U) Coast Guard Implementation of Presidential Policy Directive/PPD-28- Policies and Procedures, available at <https://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties> (mid-way through the page).
- (U) NRO Presidential Policy Directive 28 Procedures, available at <https://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties> (mid-way through the page).
- (U) Department of Energy Office of Intelligence and Counterintelligence, DOE-IN Policy Guidance Number 28.1, Implementation of PPD-28, available at <https://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties> (mid-way through the page).
- (U) Email from CIA Privacy and Civil Liberties Officer Benjamin Huebner to PCLOB Board Member Elisebeth Collins (December 7, 2016).