[redacted]

Contains deliberative information

PRIVACY & CIVIL LIBERTIES OVERSIGHT BOARD

[redacted] REPORT ON CIA FINANCIAL DATA ACTIVITIES IN SUPPORT OF ISIL-RELATED COUNTERTERORRISM EFFORTS

(U) CONTENTS

[redacted]

[redacted]

(U) INTRODUCTION

A. (U) The Privacy and Civil Liberties Oversight Board

(U) The Privacy and Civil Liberties Oversight Board ("PCLOB") is an independent agency within the executive branch, established by the Implementing Recommendations of the 9/11 Commission Act of 2007.[1] The bipartisan, five-member Board is appointed by the President and confirmed by the Senate. The PCLOB's mission is to conduct oversight and provide advice to ensure that efforts by the executive branch to protect the nation from terrorism are appropriately balanced with the need to protect privacy and civil liberties.

(U) In its oversight role, the Board is responsible for continually reviewing executive branch policies, procedures, regulations relating to efforts to protect the nation from terrorism, and their implementation, in order to ensure that privacy and civil liberties are protected. The Board also is responsible for continually reviewing executive branch information-sharing practices and any other actions of the executive branch relating to efforts to protect the nation from terrorism, in order to determine whether such actions appropriately protect privacy and civil liberties and whether they are consistent with governing laws, regulations, and policies regarding privacy and civil liberties.[2]

B. (U) The Board's examination of Executive Order 12333 activities

(U) In July 2014, the Board announced that it would review, among other matters, counterterrorism-related intelligence activities conducted pursuant to Executive Order 12333, as amended ("E.O. 12333"). First issued in 1981 and last updated in 2008, E.O. 12333 establishes an operational framework for 17 federal entities designated as part of the nation's Intelligence Community ("IC").[3] The executive order does not provide authority for any one intelligence-gathering effort, nor is there any single E.O. 12333 surveillance "program." Yet, understanding how IC elements implement E.O. 12333 is a critical part of understanding how entities balance the need to protect privacy and civil liberties with the need to protect the nation against terrorism. The order regulates the use of certain intelligence-gathering methods and outlines parameters under which intelligence agencies may collect and utilize information about United

1 (U) Pub. L. No. 110–53, § 801, 121 Stat. 266, 352 (2007).
2 (U) 42 U.S.C. § 2000ee(d)(2).
3 (U) Executive Order 12333 was signed on December 4, 1981. It was amended in 2004 by Executive Order 13355 to facilitate "strengthened management of the Intelligence Community." Executive Order 12333 was again amended in 2008 by Executive Order 13470 to strengthen the role of the Director of National Intelligence and permit the sharing of signals intelligence under certain conditions.

States persons ("USPs").[4] Among other things, E.O. 12333 requires IC elements to issue and follow procedures approved by the Attorney General in order to collect, retain, or disseminate information concerning USPs, or use certain collection methodologies within the United States or directed at USPs abroad.[5]

(U) In April 2015, the Board adopted a project description memorializing its approach to its E.O. 12333 oversight effort. The Board explained that it would select specific counterterrorism-related activities conducted under E.O. 12333 by the Central Intelligence Agency ("CIA") and National Security Agency ("NSA"), and would conduct in-depth examinations of those activities. The Board further explained that it would issue a public report that explains how the legal framework established by the executive order and its implementing procedures governs the collection, use, retention, and dissemination of information concerning U.S. persons.[6]

(U) Later in 2015, the Board selected for in-depth examinations three sets of counterterrorism-related activities conducted under E.O. 12333: two sets of activities conducted by the CIA and one set conducted by the NSA. This report regards one of the two in-depth examinations of certain CIA counterterrorism activities.

(U) On January 3, 2017, the Board voted unanimously to adopt this report. Board Members Wald and Dempsey wrote a joint separate statement, which is appended to this report.

C. (U) Purpose and focus of this report

[redacted]This report examines the CIA's financial data activities conducted under E.O. 12333 in support of counterterrorism efforts with respect to the network of the Islamic State in Iraq and the Levant, or ISIL— an entity that the State Department has designated as a terrorist organization.[7] In July 2015, the Board selected this topic for an in-depth examination. By focusing on this area, the Board has been able to review certain CIA activities in the context of a current and ongoing terrorist threat.

[redacted]Thus, the review covers "financial intelligence activities" which includes a variety of information derived from financial data. This data can illustrate the flow of funds used by

[4] (U) A "United States person" under E.O. 12333 means (1) "a United States citizen," (2) "an alien known by the intelligence element concerned to be a permanent resident alien," (3) "an unincorporated association substantially composed of United States citizens or permanent resident aliens," or (4) "a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments." Exec. Order No. 12333 § 3.5(k).

[5] (U) Exec. Order. No. 12333 § 2.3-2.4.

[6] (U) "PCLOB Examination of E.O. 12333 Activities in 2015," *available at* https://www.pclob.gov/library/20150408-EO12333_Project_Description.pdf.

[7] (U) Office of the Spokesperson, U.S. Dep't of State, "Terrorist Designations of Groups Operating in Syria" (May 14, 2014). For the purposes of this report, the Board uses the phrase "counterterrorism efforts" to refer to "efforts to protect the Nation against terrorism." *See generally* 42 U.S.C. § 2000ee(d)(2).

[redacted]

[redacted]

terrorist organizations, the connections among individuals in terrorist networks, and detailed information about the individuals supporting terrorist organizations. [redacted]

[redacted]

[redacted]In this examination, the Board focused on a particular set of CIA foreign financial intelligence activities under a particular legal framework: the collection, retention, analysis, and dissemination of financial data pursuant to E.O. 12333. This examination did not explore activities conducted pursuant to specialized statutory regimes or inter-agency agreements.[12] The Board researched other government initiatives to collect financial data for intelligence purposes only for two limited reasons: (1) to understand the context in which the CIA has carried out its

---

8 [redacted]

9 [redacted]

[redacted]

11 (U//FOUO) CIA and PCLOB discussion, 8/24/16; CIA and PCLOB discussion, 8/18/16.

12 [redacted] The CIA generally considers E.O. 12333 rules to apply across its activities, including activities involving USPs or USP information, though statutory or other requirements may supplement E.O. 12333. CIA and PCLOB discussion, 9/8/15; CIA and PCLOB discussion, 4/21/15; CIA, *CIA Accuracy Review of PCLOB Notes from CIA Briefings on E.O. 12333 Rules* , Statement 1 (May 10, 2016). [redacted]

[redacted]For the purposes of this review, terms such as "E.O. 12333 activities" will refer to activities conducted under the E.O. 12333 framework and not also under a specialized collection, retention, or dissemination regime. The Board recognizes, however, that even E.O. 12333 activities may be governed by other general statutes that are beyond the scope of this review. One example of such a general statute is the Privacy Act of 1974, 5 U.S.C. § 552a, which can affect dissemination protocols *See generally* CIA and PCLOB discussion, 7/6/16.

[redacted]

E.O. 12333 financial intelligence activities, and (2) to understand the different types of privacy and civil liberties protections that have been applied in the contexts of other intelligence efforts.

The Board's examination additionally focused on a particular CIA component: . mission is to collect, analyze, and disseminate financial intelligence, a term the CIA defines as "intelligence derived from financial data that provides insight into the identities, activities, and relationships of intelligence targets."[13]

Further, the Board focused on collection activities directed against foreign entities abroad primary operational mission; however, given the global presence of USPs, handles the data assuming that it may contain incidental collection of information about USPs.[14] Though these foreign collections account for the majority of collections manages and retains under E.O. 12333,[15] These activities may include open-source research (*e.g.*, an Internet search) or inquiries to other U.S. government agencies or foreign entities.[16] Though the Board obtained policies relevant to the handling of such collections, the Board did not discuss with the CIA the details of its practices regarding such activities and so limited its review to collections acquired by targeting foreign persons or entities.

Thus, the Board's examination focused on the following: collection, processing, retention, and dissemination of financial data collected through operations directed against foreign entities and assumed to potentially contain incidentally collected USP information,[17] pursuant to E.O. 12333, to the extent that such activities are or can be part of counterterrorism efforts against ISIL. This report will use the term "covered activities" to refer to these activities.

(U) In reviewing the covered activities, the Board concentrated on the protection of U.S. persons' privacy and civil liberties. This focus on USPs is consistent with Section 2 of E.O. 12333, which contains the order's principal privacy and civil liberties protections and which centers on USPs and activities within the United States.

D. (U) Methodology

The Board's oversight was informed by briefings from and other discussions with CIA staff that took place between April 2015 and August 2016. At these briefings and other

---

13

14 (U//FOUO) CIA and PCLOB discussion, 7/6/16.

15 (U//FOUO) CIA and PCLOB discussion, 7/6/16.

16 (U//FOUO) CIA and PCLOB discussion, 8/24/16; CIA and PCLOB discussion, 8/18/16.

17 (U) This report uses term "USP information" to refer to (a) "information concerning United States persons," a term used in E.O. 12333, and (b) "information about a U.S. person," a term used in the CIA's AG-approved procedures for implementing sections of E.O. 12333.

[redacted]

sessions, the CIA staff informing the PCLOB were primarily managers and attorneys [redacted] The Board also received relevant documents from the CIA, the CIA Office of the Inspector General, [redacted]

This report follows a [redacted] report of the CIA Office of the Inspector General ("CIA OIG") [redacted] The Board understands that the CIA OIG is monitoring the CIA's response to the report's [redacted] recommendations,[19] and that the CIA has implemented many of CIA OIG's recommendations [redacted] where relevant.[20] While the CIA OIG report focused on compliance with key aspects of E.O. 12333, [redacted] and certain other CIA policies, this report focuses on how aspects of the CIA's practices protect the privacy and civil liberties of USPs.[21] Due to the CIA OIG's attention to access controls, however, the Board did not focus on access controls in this review, though the discussion below includes some key facts on the topic.

[redacted] Sections II and III below provide background on the activities that the Board reviewed and the financial data that those activities involved. Section III further discusses the covered activities in detail, including the applicable authorities. In Section IV, the Board evaluates the covered activities and identifies six recommendations for improvements in the CIA's practice.

(U) Following the Board's analysis and recommendations, this report includes a separate statement.

---

[18] [redacted] OFFICE OF INSPECTOR GEN., CIA, REPORT OF [redacted] (hereinafter "OIG Report"); CIA and PCLOB discussion, 7/6/16.

[19] [redacted] OFFICE OF INSPECTOR GEN., CIA, [redacted].

[20] [redacted] CIA and PCLOB discussion, 7/6/16; E-mail from Office of the Inspector General, CIA, to Executive Director, PCLOB (Nov. 29, 2016). According to the OIG, CIA has completed actions for [redacted] recommendations and all of the non-significant recommendations in the OIG report. CIA continues to work toward addressing [redacted] recommendations of the OIG's [redacted]

[21] [redacted] OIG Report [redacted]

[redacted]

[redacted]

II. [redacted] OVERVIEW: FINANCIAL INTELLIGENCE AND KEY AUTHORITIES

[redacted] This section provides background on the activities that the Board reviewed. Parts A through C describe financial intelligence generally, its significance, [redacted] role regarding E.O. 12333 financial data, and the use of such data in efforts related to ISIL. Part D describes key authorities applicable [redacted] E.O. 12333 financial intelligence activities, while Part E discusses the extent [redacted] trains its personnel on these authorities.

A. [redacted] Description of [redacted] E.O. 12333 financial intelligence

[redacted] groups its E.O. 12333 financial intelligence into two categories: aggregate financial data, and narrative foreign intelligence ("FI"). The former is further divided into two categories: structured data and unstructured data.[22]

[redacted] Structured data consists of data sets that can be transformed into a common format [redacted]

[redacted]

[22] [redacted]

[23] [redacted] CIA and PCLOB discussion, 8/24/16; CIA and PCLOB discussion, 8/18/16.

[24] (U//FOUO) CIA and PCLOB discussion, 11/16/15.

[redacted]

[redacted]

[redacted]

[redacted]Unstructured data can include a wide range of types of information, often captured in emails, spreadsheets, word processing files, or other electronic documents. [redacted]

[redacted]

[redacted]Narrative foreign intelligence consists of the CIA's documentation, for CIA or other audiences, of answers to specific intelligence questions[redacted]. Unlike structured or unstructured data[redacted] generally stores without systematically determining whether it constitutes foreign intelligence or other information valuable to the CIA, narrative foreign intelligence includes information that CIA personnel have already deemed to constitute foreign intelligence. Narrative FI represents an assessment by the CIA that the information is appropriate for distribution. Sometimes, a CIA officer can generate narrative foreign intelligence by documenting information directly from a conversation with a human source. In other cases, a CIA officer may generate narrative foreign intelligence after distilling other data.[29]

[redacted]Among the E.O. 12333 collections[redacted] retains, the great majority are comprised of structured data.[redacted] data collections covering about [redacted] estimated that the data were either collected from or designed to capture information regarding [redacted] collections had recurred at least once

---

25 [redacted] CIA and PCLOB discussion, 9/21/15.

26 [redacted] CIA and PCLOB discussion, 7/6/16; CIA and PCLOB discussion, 4/21/16.

27 (U//FOUO) CIA and PCLOB discussion, 7/6/16.

28 (U//FOUO) CIA and PCLOB discussion, 8/18/16; CIA and PCLOB discussion, 7/6/16.

29 [redacted] CIA and PCLOB discussion, 8/24/16; CIA and PCLOB discussion, 7/6/16.

30 (U//FOUO) CIA and PCLOB discussion, 11/24/15.

31 [redacted] CIA and PCLOB discussion, 11/4/15. In this context, a "record" refers to information about a [redacted] particular person. CIA and PCLOB discussion, 8/18/16. Some records may be duplicative of others. [redacted]

32 [redacted] CIA and PCLOB discussion, 8/18/16.

[redacted]

[redacted]

[redacted] Over the course of 2015 and 2016, narrative financial intelligence and unstructured data have become an increasingly important focus [redacted] The CIA generally collects structured financial data in large quantities from the non-USP financial [redacted] platforms enable more users to search and analyze structured financial data than to search and analyze unstructured data because [redacted] restricts access to unminimized unstructured data sets.[37] Structured data enables the identification of terrorist networks and other previously unknown identifying information; however, structured data sets are resource-intensive to process and can also take a long time to collect, particularly when the targets [redacted] resulting from a human source or through exploitation of unstructured data may most efficiently answer some of the focused questions that arise in the context of counterterrorism efforts, such as questions regarding how an organization operates.[39]

[redacted] This review focuses on E.O. 12333 collection activities that are directed against non-U.S. entities and non-USPs. [redacted] however, that these collections of structured or unstructured data potentially include incidentally collected USP information.[40] [redacted]

[redacted]

---

33 [redacted] CIA and PCLOB discussion, 9/21/15. [redacted] CIA and PCLOB discussion. 8/18/16.

34 [redacted]

35 [redacted] CIA and PCLOB discussion, 8/24/16.

36 (U//FOUO) CIA and PCLOB discussion, 7/6/16.

37 (U//FOUO) CIA and PCLOB discussion, 7/6/15; CIA and PCLOB discussion, 11/24/15.

38 (U//FOUO) CIA and PCLOB discussion, 8/24/16; CIA and PCLOB discussion, 7/6/16.

39 (U//FOUO) CIA and PCLOB discussion, 7/6/16; CIA and PCLOB discussion, 9/29/15.

40 [redacted] CIA and PCLOB discussion, 8/24/16; CIA and PCLOB discussion, 8/18/16; CIA and PCLOB discussion, 7/6/16; *see also* [redacted] The briefers additionally noted that separately [redacted] explored options to initiate collections of financial data [redacted], pursuant to the E.O. 12333 framework, that do not trigger [redacted] other statutory regimes. None of the options explored, however, have resulted in the actual collection of data.

[redacted]

[redacted]

[redacted]

B. [redacted] role and E.O. 12333 financial data in the ISIL context

[redacted]With its mission to collect, analyze, and disseminate financial intelligence, [redacted] the hub of the CIA's financial intelligence expertise. [redacted]generally leads the CIA's collection efforts aimed at acquiring [redacted], developing CIA's financial data collections, and disseminating FI reporting. [redacted] closely with other CIA components who may assist in carrying out these collection activities. With assistance [redacted] also the CIA lead for processing, retaining, and disseminating structured financial data that has not yet been reviewed for potential FI. Finally, [redacted] the CIA lead for exploiting and disseminating FI reports derived from [redacted] unstructured financial data holdings. But [redacted] analysis does not represent the CIA's definitive perspective on a particular question. Two other parts of the CIA, the Counterterrorism Mission Center and [redacted] are primarily responsible for ISIL-related all-source analysis, *i.e.*, analysis that represents the CIA's definitive perspective on an ISIL-related question.[43]

[redacted]

priorities [redacted] as policymakers have continued to refine their needs and other parts of the CIA have focused their attention on some of the other priority areas.[47] Overall, [redacted] focused efforts are designed to drive collection in support of strategic policy objectives set by the

---

41 [redacted]

42 [redacted] uses to review structured data for identifying USP information. CIA and PCLOB discussion, 8/18/16. This report uses the term "identifying information" to refer to a subset of USP information. [redacted]

43 [redacted] CIA and PCLOB discussion, 7/6/16; CIA and PCLOB discussion, 11/4/15; CIA and PCLOB discussion, 10/7/15; CIA and PCLOB discussion, 9/29/15; CIA and PCLOB discussion, 9/29/15; CIA and PCLOB discussion, 8/7/15.

44 (U//FOUO) CIA and PCLOB discussion, 8/7/15.

45 [redacted]. CIA and PCLOB discussion, 8/24/15.

46 [redacted]

47 (U//FOUO) CIA and PCLOB discussion, 7/6/16.

[redacted]

[redacted]

[redacted] leaders have described the agency's [redacted] work as unusual in some aspects because CIA approaches the target [redacted] In support of both efforts, [redacted] l expertise in close collaboration with its Counterterrorism Mission Center [redacted] counterparts. Within the CIA, the Counterterrorism Mission Center tends to be the lead on efforts related to terrorist groups [redacted] team has also employed what [redacted] describes as a mix of short-term and long-term strategies; the team addresses some intelligence needs that change quickly (*e.g.*, related to Department of Defense actions) and others that require work over a more extended period of time.[50] Additionally, events [redacted] have prompted [redacted] to explore new inter-agency data-sharing arrangements. Though [redacted] receives information from other federal agencies, it has not routinely done so on a systematic basis.[51] [redacted] now piloting two programs to receive and use [redacted] data sets that relate [redacted] The programs come with program-specific restrictions that build upon E.O. 12333 rules, and thus the programs are not a focus of this review.[53]

[redacted] Despite these unique aspects of its ISIL-related work, however, [redacted] described its processes and procedures related to ISIL as common to other CIA efforts.[54] Therefore, the Board understands the policies and practices [redacted] described to be, in large part, applicable to other [redacted] CIA efforts.

[redacted] In addressing ISIL-related priorities, [redacted] has looked both to E.O. 12333 data and to other financial information. [redacted]

---

48 [redacted] CIA and PCLOB discussion, 8/24/16.

49 [redacted] CIA and PCLOB discussion, 7/6/16. That arrangement developed at the same time that the organization was adjusting to a reorganization. *Id.*; CIA and PCLOB discussion, 5/4/15.

50 (U//FOUO) CIA and PCLOB discussion, 7/6/15.

51 [redacted] CIA and PCLOB discussion, 7/6/16; [redacted]

52 CIA and PCLOB discussion, 7/6/15; [redacted]

53 (U//FOUO) CIA and PCLOB discussion, 8/18/16.

54 (U//FOUO) CIA and PCLOB discussion, 10/7/15.

[redacted]

[redacted]

[redacted] has explained that its general practice is to use existing collections when possible, in order to limit the risks involved in obtaining new collections [redacted] expected that data derived from E.O. 12333 activities would become increasingly important to ISIL-related efforts, [redacted] obtained more ISIL-related collections and narrative foreign intelligence.[58]

[redacted] developed such additional ISIL-related collections, and had also further reviewed and processed ISIL-related collections obtained [redacted] still important, but complemented by data from a wider array of other sources. In particular, [redacted] established and significantly increased its use of information from [redacted] operations set up [redacted] and operating with coaching [redacted] on how to identify and gather useful financial information. The units have provided information on [redacted]

55 [redacted]

56 [redacted] CIA and PCLOB discussion, 4/21/15.

57 CIA and PCLOB discussion, 12/16/15; CIA and PCLOB discussion, 9/29/15; CIA and PCLOB discussion, 4/21/15.

58 (U//FOUO) CIA and PCLOB discussion, 12/16/15.

[redacted]

[redacted]

(as well as another group of interest), providing leads to CIA field stations [redacted] and possibly assisting the U.S. Government with a terrorism-related designation. The second set of information consisted of records gathered [redacted]

[redacted]

C. [redacted] The significance of [redacted] E.O. 12333 financial data

[redacted] does not systematically assess whether and how all of the E.O. 12333 financial data it holds is utilized in conjunction with the CIA's counter-ISIL mission. However, the processes for approving some collection activities include case-by-case reviews of the benefits of particular sources.[61] The CIA also does not systematically review how it or other agencies use covered data in efforts regarding ISIL or other topics. Nor does the CIA receive uniform or routine reports back from other agencies about whether or how they have used [redacted] provided information.[62] Though a "senior review panel" may evaluate the value of any particular source of financial data as part of a reauthorization determination, the evaluations are case-specific.[63]

[redacted] holds a clear view of the value of financial data generally [redacted] training regarding structured data states that "[a]nalysis of financial data can help to identify [redacted]

---

59 [redacted] CIA and PCLOB discussion, 8/24/16; CIA and PCLOB discussion, 11/4/15. [redacted] CIA and PCLOB discussion, 8/24/16.

60 (U//FOUO) CIA and PCLOB discussion, 8/24/16.

61 (U//FOUO) CIA and PCLOB discussion, 11/24/16.

62 (U//FOUO) CIA and PCLOB discussion, 11/4/15.

63 (U//FOUO) CIA and PCLOB discussion, 11/24/15; CIA and PCLOB discussion, 11/4/15.

[redacted]

[redacted]

[redacted] CIA's Counterterrorism Mission Center provided examples including the following of how ISIL-related efforts have drawn on the CIA's E.O. 12333 financial data.[69]

64 [redacted]

65 [redacted] CIA and PCLOB discussion, 8/24/15, CIA and PCLOB discussion, 9/21/15.

66 (U//FOUO) *Cf.* CIA and PCLOB discussion, 8/24/16; CIA and PCLOB discussion, 8/18/16.

67 (U//FOUO) CIA and PCLOB discussion, 11/16/15; CIA and PCLOB discussion, 5/4/15.

68 (U//FOUO) CIA and PCLOB discussion, 11/16/15.

69 [redacted] The Board received a briefing on these examples of [redacted] actions but did not review related files or otherwise examine the details of when and how financial information contributed to the actions that the CIA briefers described.

[redacted]

[redacted]

[redacted]

[redacted]

[70] (U//FOUO) CIA and PCLOB discussion, 11/16/15.

[71] [redacted] CIA and PCLOB discussion, 8/24/16; CIA and PCLOB discussion, 12/16/15; CIA and PCLOB discussion, 11/16/15.

[72] [redacted] CIA and PCLOB discussion, 8/24/16; [redacted]

[redacted]

[redacted]

[redacted]

D. (U//FOUO) Key authorities applicable to covered activities

(U) E.O. 12333 is the overarching framework for this review. Section 1.7 of the order sets out general duties and responsibilities of the CIA, while Section 2 discusses how the CIA should conduct its intelligence activities. Within the order, Sections 2.3 and 2.4 are the most pertinent to the protection of USPs in the course of the covered activities. Section 2.3 regards the collection, retention, and dissemination of USP information. Section 2.4 discusses collection techniques and requires agencies to have specialized procedures regarding their use of particular techniques.[76]

(U//FOUO) Also relevant to this review is a cascading set of E.O. 12333-related CIA authorities, some of which have changed since the Board completed its review of covered activities. Among these authorities, three are critical. The first is Annex A to the CIA's Agency Regulation 2-2 ("AR 2-2"). During the time period covered by this examination, Annex A was one of two parts of the CIA's Attorney General-approved procedures to implement Sections 2.3 and 2.4 of E.O. 12333. AR 2-2, Annex A, covers CIA intelligence activities outside the United States, and AR 2-2Annex B covers CIA intelligence activities within the United States, which are beyond the scope of this review.[77]

---

73 [redacted]

74 [redacted]

75 [redacted]

76 (U) Other parts of Section 2 regard specialized circumstances that the CIA has not suggested apply to the covered activities.

77 (U) (6.3.1) AR 2-2A Annex A, *Guidance for CIA Activities Outside of the United States* § I.I.A (Dec. 23, 1987) (signed 1982) (hereinafter "Annex A"); (6.3.2) AR 2-2B Annex B, *Guidance for CIA Activities Within the United States* § II.I.A (Dec. 23, 1987) (updated in 2005) (hereinafter "Annex B").

[redacted]

[redacted]

(U) The second critical authority is [redacted] which concerns certain information [redacted] also must be read in conjunction [redacted] as both of these [redacted] included definitions.[78]

[redacted] The third key authority is the [redacted] collection, retention, and dissemination of "aggregate data," *i.e.*, "electronically-stored information that has the potential to contain identifying U.S. person information and is collected for operational purposes."[79] [redacted] considers both its structured and unstructured E.O. 12333 financial data to constitute "aggregate data." By contrast, [redacted] narrative foreign intelligence to be outside the definition of "aggregate data" given it is either derived from "aggregate data" or provides answers to specific questions.[80]

[redacted] officials described the [redacted] Policy as a critical touchstone for their operations.[81] The [redacted] Policy was drafted to address a perceived weakness in AR 2-2 and its annexes. [redacted] This report also cites, as appropriate, AR 2-2, the CIA regulation to which Annex A [redacted] attached. AR 2-2, which was not subject to Attorney General review and approval, summarizes and incorporates by reference key provisions of Annex A and other

---

78 [redacted]

79 [redacted] CIA and PCLOB discussion, 7/6/16.

80 (U//FOUO) CIA and PCLOB discussion, 7/6/16.

81 (U//FOUO) CIA and PCLOB discussion, 7/6/16.

82 [redacted]

83 [redacted]

[redacted]

[redacted]

annexes. The rule also implements provisions of E.O. 12333 other than sections 2.3, 2.4, and 2.9, includes related policy provisions, and summarizes key statutes that may govern CIA activities.[84]

[redacted] This report is based on these and other authorities as they were in effect through August 2016, when the Board completed its research regarding the CIA's activities. The CIA plans to adopt revised AG-approved procedures to implement Sections 2.3 and 2.4 E.O. 12333 by December 2016.[85] The revised procedures ("New Procedures") will replace Annex A [redacted] as well as Annex B to AR 2-2.[86] The New Procedures will necessitate revisions to other policies, including the [redacted] Policy.[87] This report notes the relevant changes anticipated by the new AG-approved procedures based on a preliminary draft provided to PCLOB staff, though the procedures have not yet been finalized and thus may be subject to additional edits before signature.

E. (U//FOUO) Training

[redacted] employees, case-specific consultations with embedded attorneys may be the primary source of information about legal and policy rules related to covered activities though all regulations are available online for general access. [redacted] officials explained that, in general, CIA personnel know to stop and consult attorneys if they come across USP information. In counterterrorism operations in particular, USP information may be unavoidable; to address case-specific questions related to this information, the CIA has increased its placement of attorneys to work hand-in-hand with CIA line staff.[88]

[redacted] This consultation-focused culture is reflected in the limited formal training [redacted] employees are required to receive regarding the various governing authorities relevant to covered activities. Among the trainings [redacted] provided to the Board regarding E.O. 12333 and related authorities, only one is mandatory [redacted][89] Furthermore, only some of the trainings provided include information about the [redacted] policy or the aspects of Annex A [redacted] that might apply to covered activities. [redacted]

---

84 (U) (6.3) AR 2-2, *Law and Policy Governing the Conduct of Intelligence Activities* (Dec. 23, 1987).

85 [redacted]

86 (U//FOUO) CIA and PCLOB discussion, 8/24/16. For the purposes of this draft, all cites and references to the "New Procedures" refer to the draft dated 9/22/2016 and shared with the PCLOB on 10/11/2016.

87 (U//FOUO) CIA and PCLOB discussion, 6/27/16.

88 (U//FOUO) CIA and PCLOB discussion, 7/6/16.

89 [redacted] E-mail from Benjamin Huebner, Privacy and Civil Liberties Officer, CIA, to PCLOB staff (Sept. 9, 2016); CIA, [redacted] E-mail from Benjamin Huebner, Privacy and Civil Liberties Officer, CIA, to PCLOB staff (Sept. 9, 2016); CIA and PCLOB discussion, 10/19/15.

[redacted]

[redacted]

It does not cover the collection or handling of USP information that is incidentally collected outside of the United States. Moreover, the training focuses on E.O. 12333 and high-level principles captured in AR 2-2 and its annexes. The training slides do not appear to address special rules applicable [redacted][90] Though other training materials [redacted] provided to the Board address the [redacted] Policy, those trainings are optional.[91]

[redacted] The Board understands [redacted] employees may receive job-specific training that goes beyond the materials the Board reviewed. [redacted] explained that for personnel involved in targeting and managing operations, the CIA provides "unique and rigorous training and certifications . . . that shape their decision making."[92] One example is a certification course for targeters that includes instruction on how to assess the risks and benefits of accessing a target.[93] But these trainings may not provide [redacted] personnel with a comprehensive understanding of the protections for USP information collected incidentally. The CIA OIG took a broad look at CIA trainings to identify the ones that addressed E.O. 12333 requirements including the handling of USP information. It then reviewed the training records [redacted] users within the CIA. The CIA OIG concluded that nearly half of the random sample of users and virtually all [redacted] had not completed any of the trainings that the CIA OIG had identified as addressing the requirements of E.O. 12333. However, the OIG report predates the standup of [redacted] and does not reflect the current training requirements [redacted][94]

III. [redacted] FINANCIAL DATA PROCESSES

[redacted] This section discusses [redacted] conducts financial intelligence activities that can be used in counterterrorism efforts regarding ISIL. Each of Parts A through C discusses the practice and policies that the Board reviewed in 2015 and 2016, and concludes with a discussion of the New Procedures that are being finalized and are anticipated to be approved in December 2016.

90 [redacted].

91 [redacted]

92 [redacted]

93 (U//FOUO) CIA and PCLOB discussion, 9/21/15.

94 (U) OIG Report [redacted]

[redacted]

[redacted]

A. [redacted] Collecting E.O. 12333 financial information

1. [redacted]

[redacted] describes two primary goals for the collection of financial intelligence, including both narrative FI and financial data: to collect reliable, credible information not available elsewhere that addresses key strategic intelligence gaps, and to disseminate information to the wider IC for purposes of network development and validation of targets. A new collection operation begins with targeting, the process to identify a target and the means of accessing it. [redacted] the targeting process is run by individuals called targeters, though others may assist.[95]

[redacted] conducts research to identify a target related to a known intelligence gap. High-level, ongoing intelligence needs stemming from the National Intelligence Priorities Framework ("NIPF") are used [redacted] to identify priority targets.[96] [redacted] may also receive a request from another agency to answer a specific question [redacted] could receive a lead on a potential target from a CIA field station or through research in existing holdings. [redacted] will map any identified gap to a NIPF priority and assess whether the potential target can provide information to address the gap. In any of these circumstances, the targeter will determine the priority of the potential target and the intended operational goal. [redacted] identifies a target that could fill a known intelligence gap, [redacted] pursues it.[97]

[redacted] After matching a potential target and an intelligence gap, the next steps are to research related information and then assess how the CIA could access the target. [redacted] then propose a course of action. Collection operations are carried out by other headquarters divisions, field stations, [redacted] operating at the CIA's request.[98]

[redacted] For collections of structured financial data, the target is typically a particular foreign [redacted]

---

95 (U//FOUO) CIA and PCLOB discussion, 10/7/15; CIA and PCLOB discussion, 9/21/15.

96 (U) *See generally* Intelligence Community Directive 204 (Jan. 2015) (regarding how the NIPF is used to establish and manage national intelligence priorities).

97 [redacted] CIA and PCLOB discussion, 10/7/15; CIA and PCLOB discussion, 9/21/15.

98 [redacted] CIA and PCLOB discussion, 10/7/15; CIA and PCLOB discussion, 9/21/15.

[redacted]

[redacted]

[redacted] The targets for unstructured collections are more varied. But often targets for unstructured collections are chosen with a more specific intelligence focus than the targets of structured collections. For instance, a collection of unstructured information could result from [redacted]

[redacted] In identifying a target, [redacted] focuses on filling intelligence gaps but does not have a specific standard for deciding to pursue a target. Rather the targeting decision is based on an evaluation of the type and content of information [redacted] linking the information assessed to be possessed by a potential target to an intelligence gap. [redacted] evaluates a number of aspects of an operation in addition to the strength of the information pointing toward a potential target. [redacted] emphasized that the group's goal of collecting credible information in a safe way focuses staff on priority needs. [redacted] routinely analyzes a new operation's potential benefits and risks, including risks to human sources [redacted] targeting decisions also can reflect the difficulty of reaching certain targets or types of targets. [redacted] emphasized that in the context of counterterrorism operations, [redacted] significant amount of time and counterterrorism work requires keeping up with terrorist organizations that may constantly change [redacted]

[redacted] Practical considerations also shape the breadth of an operation. In proposing an operation, [redacted] provides instructions about the type of data that most interests [redacted] For structured collections, those instructions generally focus on [redacted] data. The officers carrying out the operation will attempt to focus their efforts accordingly. However, the exact scope of the operation will depend on factors including the duration of the source's access to the records and how easily the source can identify the prioritized records.[102]

---

99 [redacted] E-mail from Office of Privacy and Civil Liberties, CIA, to PCLOB staff (May 25, 2015); CIA and PCLOB discussion, 8/18/16; CIA and PCLOB discussion, 7/6/16.

100 (U//FOUO) CIA and PCLOB discussion, 8/18/16.

101 (U//FOUO) CIA and PCLOB discussion, 8/18/16; CIA and PCLOB discussion, 10/7/15.

102 [redacted] CIA and PCLOB discussion, 8/24/16; CIA and PCLOB discussion, 8/18/16; CIA and PCLOB discussion, 10/7/16. [redacted] CIA and PCLOB discussion, 8/18/16.

[redacted]

[redacted]

[redacted] lawyer emphasized that the CIA often has an interest in getting additional relevant information where possible.[103] For instance, in response to a [redacted] instruction to focus [redacted][104] In carrying out this type of collection, the CIA may acquire other information that the CIA considers to be of potential intelligence value, [redacted]

[redacted] officials also emphasized that targeters try to limit the amount of information about USPs that is collected.[105] [redacted] examples of such limits focus on avoiding information that is clearly identifiable as U.S.-focused. For example, [redacted] stated that CIA operators would try to avoid collecting information [redacted] believed to have a connection to the United States. Similarly, [redacted] CIA operators would try to avoid [redacted] asserts that it follows routine steps to limit USP data.

[redacted] Opportunities to clearly identify and avoid USP information may not exist. [redacted] advises that under some circumstances, personnel do not have adequate information, ability, or opportunity to reduce collection of USP information by limiting the scope of the collection. [redacted] does not attempt to estimate ahead of time how *much* USP information a particular collection will likely involve, in many cases because it is not possible to make such an estimate.[106]

[redacted] Before proceeding forward, [redacted] proposed activity goes through a multi-layered approval process. The process includes [redacted] management and other CIA offices with interests in the activity, such as the Counterterrorism Mission Center [redacted] for an operation directed [redacted]. In reviewing a proposed activity, a headquarters office may reject a proposed collection activity, for reasons such as the existence of an alternative mechanism to obtain or access the sought-after information. With headquarters

---

103 (U//FOUO) CIA and PCLOB discussion, 9/17/15.

104 (U//FOUO) CIA and PCLOB discussion, 8/18/16; [redacted]

105 [redacted] CIA and PCLOB discussion, 7/6/16.

106 (U//FOUO) CIA and PCLOB discussion, 10/7/15.

[redacted]

[redacted]

approval, [redacted] sends the description of the activity to the relevant field station or headquarters office to decide whether and when to implement it based on resource and other considerations.[107]

[redacted]During the approval process, issues related to USPs may be raised, but the mechanisms for doing so vary according to the type of proposed operation [redacted] the standard approval cable must document USP-related issues, including whether there is a chance of collecting information regarding a USP. [redacted] approval cables do not use a standard format that ensures USP issues are documented. Collectors, however, are taught to highlight any issues related to USPs in cable traffic and responding guidance is documented in a cable response.[108]

[redacted] representatives stated that the group aims to have a lawyer review every (or nearly every) collection proposal. But CIA documents suggest that lawyers are not required to be involved in every approval process. PCLOB staff was informed that attorney review does not routinely include a detailed written analysis [redacted]

[redacted]Once a collection activity is approved, the timeline for initiating and carrying out the new activity can vary widely, depending on, among other things, the collection method.[109]

[redacted]The operations that follow the targeting process result in both unstructured and structured data that come from a variety of sources. For example, though most structured information may [redacted] a small portion [redacted] structured data (as well as its unstructured data) is drawn [redacted]

---

107 [redacted] CIA and PCLOB discussion, 8/18/16; CIA and PCLOB discussion, 10/7/15; CIA and PCLOB discussion, 9/21/15.

108 [redacted] CIA and PCLOB discussion, 8/18/16; CIA and PCLOB discussion, 10/7/15. [redacted] templates for approval cables that are specific to the type of operation. The Board received, as an example, the template for the cable approving [redacted]

109 (U//FOUO) CIA and PCLOB discussion, 10/7/15.

110 (U//FOUO) CIA and PCLOB discussion, 7/6/16; CIA and PCLOB discussion, 12/16/15; CIA and PCLOB discussion, 9/29/15.

[redacted]

[redacted]

estimated that more than half [redacted] data collections it held [redacted]

[redacted]

[redacted] methods for collecting financial information also vary. The group's financial data holdings include information collected through [redacted]

[redacted] When the CIA [redacted] may conduct some research to evaluate the value of the information in the context of CIA's national security mission and collection needs. But even if the research turns up little information, [redacted]

[redacted]

2. [redacted] Key rules regarding collection [redacted]

[redacted] identification of targets and management of operations takes place against the backdrop of E.O. 12333, AR 2-2 and accompanying Annex A, [redacted] along with the [redacted] Policy. Each of these sources provides guidance on the conduct [redacted] intelligence activities including permissible collection techniques, approvals necessary for commencement of a particular operation, and retention and dissemination of information acquired as a result of that operation. [redacted]

[redacted]

[redacted] Section 2.3 of E.O. 12333 lists ten types of information concerning USPs that IC elements can collect. Such collection may only be conducted subject to specific AG-approved procedures. The CIA considers the list in Section 2.3 to be exclusive, and it thus operates as a key limit on collections of USP information.[115] Sections 2.4 and 2.5 of E.O. 12333 also limit the

---

111 [redacted] CIA and PCLOB discussion, 12/16/15. [redacted] CIA and PCLOB discussion, 8/24/15.

112 [redacted] CIA and PCLOB discussion, 9/21/15.

113 (U//FOUO) CIA and PCLOB discussion, 9/21/15.

114 [redacted] *CIA Accuracy Review of PCLOB Notes from CIA Briefings on E.O. 12333 Rules*, Statement 92 (May 10, 2016); CIA and PCLOB discussion, 9/8/15.

115 (U//FOUO) *CIA Accuracy Review of PCLOB Notes from CIA Briefings on E.O. 12333 Rules*, Statement 72

[redacted]

techniques that can be used to collect USP information. The limits include a requirement to use the "least intrusive collection techniques feasible within the United States or directed against United States persons abroad." Annex A implements E.O. 12333's "least intrusive collection technique" requirement regarding activities outside of the United States involving U.S. persons.[116] Given that the Executive Order's restriction only applies to activities in the United States or activities directed against U.S. persons abroad, the CIA interprets the language of Annex A to only apply to collections directed against USPs abroad. Annex A does not require to apply the least intrusive collection technique to collections covered by this report, which are generally not directed against USPs.[117]

Annex A implements the E.O. 12333 protections by directing that collection activities must be related to identified CIA responsibilities. view, typically, two protections in Annex A are applicable to the covered activities: (1) the general instruction for collections to be related to CIA responsibilities, and (2) guidance regarding collection and processing of incidentally acquired USP information.[118] Annex A further divides collection activities directed against USPs [119] This tiered approach represents one of Annex A's key collection-specific protections for USPs. The CIA considers the framework to represent increasing levels of intrusiveness and Annex A requires increasing levels of approval for each category.[120]

does not generally direct collections against USPs, and Annex A does not expressly address bulk or non-targeted collections, attorneys look to the Policy for guidance. Policy supplements E.O. 12333 and any applicable Annex A rules with two collection limits. First, the policy requires that any acquisition of aggregate data be approved by group management, which in this case means management.[121] The policy lists elements that must be documented with approval, including the purpose, target, location, technique, risks and benefits, and details regarding the content, including how a source originally acquired the data.[122] Second, unlike either E.O. 12333 or Annex A, the policy addresses the scope of a collection. It requires "reasonable steps to limit the inadvertent collection of non-pertinent information that is of little or no intelligence value,

(May 10, 2016).

116 (U) Annex A § I.IV.D.

117 (U) E.O. 12333 §§ 2.4, 2.5; Annex A § I.IV.A, D.

118 (U) Annex A §§ II, III, VI.

119

120 *CIA Accuracy Review of PCLOB Notes from CIA Briefings on E.O. 12333 Rules*, Statement 6 (May 10, 2016); CIA and PCLOB discussion, 9/17/15; CIA and PCLOB discussion, 4/21/15.

121

122

[redacted]

particularly identifying U.S. person information that does not constitute foreign intelligence and is not otherwise appropriate for permanent retention consistent with Executive Order 12333 and HR 7-1 [now AR 2-2].” The policy gives two examples of “reasonable” steps. First, “personnel should acquire the smallest separable subset of data containing the information necessary to achieve [redacted] intelligence collection mission.” Second, “where practicable . . . personnel should employ filters, or similar technology, in order to limit the acquisition of information not required to fulfill CIA’s mission objective.”[123]

[redacted] As described above, [redacted] practices include the group management approval that the [redacted] Policy requires. The template for a technical operations approval cable appears to include the categories of information that the [redacted] Policy requires to be documented as a condition of approval.[124]

[redacted] management views the [redacted] Policy’s instruction on limiting incidental and inadvertent collection as a general directive regarding the breadth of a collection.[125] [redacted] does not have a prescribed set of steps to address the [redacted]Policy’s instructions. Instead, as described above, a variety of practical considerations, as well as concerns about USP information, shape the breadth of a collection.[126]

[redacted]

collections be made with discriminants when practicable,[129] and requires that [redacted] tailoring requirement be implemented “by means of the least intrusive technique required to obtain intelligence of the nature, reliability, and timeliness required.”[130] Unlike the “least intrusive technique” requirement in E.O. 12333 and Annex A, the CIA guidance implementing

123 [redacted]

124 [redacted]

125 (U//FOUO) CIA and PCLOB discussion, 8/18/16; [redacted]

126 [redacted] CIA and PCLOB discussion, 11/4/15. [redacted] CIA and PCLOB discussion, 7/6/16; CIA and PCLOB discussion, 9/21/15.

127 [redacted]

128 [redacted]

129 [redacted]

130 [redacted]

[redacted]

[redacted] limit this requirement to collections within the United States or directed at USPs abroad.[131]

[redacted] In applying the above requirements, [redacted] focuses on pre-collection controls. [redacted] has no routine mechanisms for auditing or checking compliance with legal requirements or other rules after a collection is completed [redacted] officials describe problems as generally caught before a collection is initiated, and they cite day-to-day interaction with staff and inspections by the CIA Office of the Inspector General as other measures for identifying problems.[132]

3. (U//FOUO) New AG-approved procedures

[redacted] CIA officials describe the New Procedures as addressing a gap in Annex A regarding information about USPs that is incidentally collected [redacted] the New Procedures state that "[u]nevaluated information is presumed to include incidentally acquired information concerning U.S. persons, and to be subject to these Procedures regardless of the location of the initial collection, unless the CIA obtains specific information to the contrary."[134] They also expressly permit the collection of incidentally acquired information concerning USPs.[135]

[redacted] Similar to Annex A, the New Procedures' collection-related protections for USPs focus on collections within the United States or directed at USPs. The New Procedures require approvals for collections directed at USPs or for bulk and certain other collection activities under Section 5. CIA officials may use a collection technique directed at a USP only if a less intrusive technique cannot acquire intelligence "of the nature, reliability, and timeliness required."[136]

[redacted] The New Procedures include several provisions that could formalize existing CIA practice or provide additional protections for incidentally acquired USP information, depending in part [redacted] interpret and implement them. First, the procedures would expressly require that collections fall within one of the categories named in Section 2.3 of E.O.

---

131 [redacted] Annex A §§ I.IV.D, I.V.B-D *and* E.O. 12333 § 2.4.

132 (U//FOUO) CIA and PCLOB discussion, 7/6/16.

133 [redacted]

134 (U//FOUO) New Procedures §§ 3.2 (emphases omitted), 4.2. The New Procedures define "unevaluated information" as information that has been collected but not yet reviewed for various aspects. The definition states that any collection "may produce unevaluated information" and that "unevaluated information is generally presumed to contain incidentally acquired information concerning U.S. persons, regardless of the location of collection." § 12.22 (emphases omitted).

135 (U//FOUO) New Procedures § 4.1.

136 (U//FOUO) New Procedures § 4.1.

[redacted]

[redacted]

12333.[137] Second, the procedures limit collections to "the amount of information reasonably necessary" to support the purpose of collection.[138] Third, the procedures expressly prohibit collections concerning U.S. persons "solely for the purpose of monitoring (1) activities protected by the First Amendment or (2) the lawful exercise of rights secured by the Constitution or laws of the United States."[139] Fourth, the procedures require documentation for certain collections: (1) collections made without discriminants, which the procedures term "bulk collection," and (2) collections that are so large that the CIA either cannot evaluate them promptly or evaluates a collection as a whole, without individualized review of the data.[140]

[redacted]For these bulk or large collections, the New Procedures require documentation of collection similar to that required by the [redacted] Policy: the purpose, the location (including how a source originally acquired the data), and the technique of the collection must be documented.[141] The New Procedures also require documentation of several aspects of these collections that go beyond [redacted] has described as routine under its 2015 and 2016 practices.[142]

[redacted] First, CIA officials must state, in writing, either (1) "[t]hat the collected information . . . meets the retention criteria" of the New Procedures without individualized review of the data, or (2) "that the collected information (or a subset thereof) will be stored and handled as unevaluated information."[143] Statements regarding the latter must also indicate whether the information is anticipated to include USPII that is substantial in volume, proportion, or sensitivity and whether the collected information is subject to exceptional or routine handling and querying requirements.

[redacted]Second, CIA officials must describe how the responsible CIA office "will implement any applicable handling and querying requirements."[144]

[redacted]Third, when documenting which collection techniques CIA employed, CIA officials must indicate "any reasonable steps that were or will be taken to limit the information to the smallest separable subset of data containing the information necessary to achieve the purpose of the collection."[145] Unlike the [redacted] Policy, however, the New Procedures do not expressly require personnel to *take* such "reasonable steps." The New Procedures' guidance on

---

137 (U//FOUO) New Procedures §§ 2.3, 4(a).

138 (U//FOUO) New Procedures § 3.3.

139 (U//FOUO) New Procedures § 3.3.

140 (U//FOUO) New Procedures §§ 5.1, 5.2; *see also* § 12.2 (defining "bulk collection").

141 (U//FOUO) New Procedures § 5. 2(a), (b), (c).

142 [redacted] CIA and PCLOB discussion, 10/7/16.

143 (U//FOUO)New Procedures § 5.2(d).

144 (U//FOUO) New Procedures § 5.2 (e).

145 (U//FOUO) New Procedures § 5.2(c); *see also* §§ 12.11 (defining "evaluated information"), 12.22 (defining "unevaluated information").

[redacted]

[redacted]

what constitutes reasonable steps is similar [redacted] though the two documents reflect some differences.[146]

B. [redacted] Processing and retention of E.O. 12333 financial information

[redacted] When CIA components collect E.O. 12333 financial data, they generally send it to [redacted] staff process new data sets: they categorize them, load them onto networks, and take other steps both to make the information accessible for users and to protect USP information.[147] Along the way, the financial data information is "retained"—a term that CIA officers and CIA policies use in varying ways but this report uses to refer to any CIA storage of information received by CIA headquarters.

[redacted] processing generally begins with the [redacted] receipt of a [redacted] Cable that describes the collection and type of information that is being sent [redacted] the form seeks details on the collection, such as the number of files collected, as well as the acquisition and sourcing, including the target, the involvement of other entities, and the related NIPF topic. [redacted] The form does not, however, ask for categorization of collections according [redacted] framework. In other words, it does not include a space for a CIA officer to indicate whether a collection is basic, standard, or special or that a collection does not trigger [redacted] framework. Nor does the form ask whether a collection constitutes [redacted]

[redacted] Based on the [redacted] identifies whether or not a collection is financial, and loads it electronically onto [redacted]

146 (U//FOUO) *Compare* New Procedures § 5.2(c) [redacted]

147 [redacted] CIA and PCLOB discussion, 11/4/15.

148 [redacted]

149 [redacted] E-mail from Office of Privacy and Civil Liberties, CIA, to PCLOB staff (May 23, 2015) [redacted] "CIA Documents Provided to the PCLOB For the Executive Order 12333 Deep Dives" (May 23, 2015) [redacted]

150 [redacted].

151 [redacted] CIA and PCLOB discussion, 8/18/16.

152 [redacted] CIA and PCLOB discussion, 8/24/16; CIA and PCLOB discussion, 7/6/16; CIA discussion with PCLOB, 11/24/15; CIA discussion with PCLOB, 11/4/15. The CIA OIG report describes a different path for data; it states that only [redacted] collections [redacted] and that all other collections [redacted]

[redacted]

[redacted]

generally documents the new financial collections [redacted] though that practice has included some gaps because collections owned by other CIA offices are captured in other, complementary databases.[153]

[redacted]After a collection is loaded,[redacted] first steps are to assess the structure of the information. If the data format suggests that the data consists [redacted] or other material distinct from financial data,[redacted] may route the data [redacted] for processing and loading onto a system with similar non-financial information.[154] [redacted] concludes, however, that the collection really is financial data, [redacted]will continue processing it, based on the assessment of [redacted] subject matter expert regarding the content and processing options.[155] After this point, the practices for processing and retaining E.O. 12333 financial information depend primarily on whether the information is structured or unstructured, as well as the information's source. A third set of practices apply to narrative financial intelligence, which field stations may document directly or [redacted] may derive from structured or unstructured information.[156] The systems for processing and retaining narrative financial intelligence [redacted] however, and the Board has not examined them in detail. Section C below discusses [redacted] intelligence as one form of dissemination.

1. [redacted] practice regarding structured information

[redacted]

[redacted] Making a new data set accessible [redacted] requires several steps that together [redacted] depending on the technological

---

[redacted]

153 [redacted] CIA discussion with PCLOB, 11/24/15; CIA discussion with PCLOB, 11/4/15. [redacted] CIA officials concurred with recommendations to address that gap. OIG Report [redacted]

154 [redacted] CIA and PCLOB discussion, 11/16/15; CIA and PCLOB discussion, 11/4/15.

155 [redacted]

156 (U//FOUO) CIA and PCLOB discussion, 8/24/16; CIA and PCLOB discussion, 7/6/16.

157 (U//FOUO) CIA and PCLOB discussion, 8/18/16; CIA and PCLOB discussion, 7/6/16.

158 [redacted]

[redacted]

requirements.[159] assesses whether the data contains enough content to meet the minimum standards if, for example, the data set includes names but no other accompanying identifiers, will not generally load the data though it may make exceptions in certain cases.[160] tests whether the data fields match the model. If so, team transforms the data to fit—a step that can be time-consuming if the data format is complicated runs the automated algorithm that identifies records containing presumed USP identifying information masks fields containing personally identifiable information that has been identified In these masked fields, retains the underlying information, but the text available to the user reads "*Restricted" such that user will not be able to ascertain the USP identifying information simply from reviewing the record.[162]

2. practice regarding unstructured information

Unlike structured data, unstructured E.O. 12333 financial data remains on the network where it was originally loaded: does not run on these data sets or otherwise mask USP information; by definition, unstructured data is not compatible with such automated review.[163]

receives unstructured data, the group's exploiters begin assessing the new information for its value. Since launch in March has introduced new processes through which the group immediately assigns a subject matter expert to each new collection. managers describe subject matter expertise as particularly important in reviewing unstructured data, which may be in a foreign language and, by definition, does not

---

159 (U//FOUO) CIA and PCLOB discussion, 8/24/16.

160 (U//FOUO) CIA and PCLOB discussion, 11/4/16.

161 CIA and PCLOB discussion, 8/24/16; CIA and PCLOB discussion, 11/4/15;

162 E-mail from Benjamin Huebner, Privacy and Civil Liberties Officer, CIA, to PCLOB staff (Sept. 16, 2016); CIA and PCLOB discussion, 11/4/15. The CIA OIG reviewed the filters used and related procedures and concluded that they are "effective in identifying USP information in bulk financial data." OIG Report . The CIA OIG described a separate process by which the CIA's takes steps to "minimize," *i.e.*, delete, segregate, or mask USP information in certain collections before the data is transferred. OIG Report the only algorithm that it applies to structured financial data. CIA and PCLOB discussion, 8/18/16.

163 CIA and PCLOB discussion, 8/18/16; CIA and PCLOB discussion, 7/6/16.

[redacted]

have the recognizable format of structured data.[164] With an unstructured data set, the expert first reviews the collection for its gist, conducts rough translation of key materials if needed, and flags files of interest for other colleagues. Eventually, the expert[redacted] personnel will review the information more thoroughly for foreign intelligence value, have the information fully translated if needed, and distribute appropriate information through narrative FI reports.[165]

3. [redacted] Key rules regarding processing and retention [redacted] implementation

[redacted] E.O. 12333, Annex A, [redacted] Policy address the CIA's retention of USP information. [redacted] authorities may also be relevant to[redacted] processing and retention [redacted]

[redacted] In Section 2, E.O. 12333's key limit on the retention of USP information is its list of categories of USP information that IC elements can retain under AG-approved procedures. The categories are the same as those listed for collection (and dissemination). As noted earlier, the CIA considers the list to be exclusive.

[redacted] In implementing this E.O. 12333 framework, Annex A not only includes the general requirement that activities be related to CIA responsibilities, but also sets out protections for USP information based on the same framework it established for collection.[168] [redacted] includes one set of retention rules for USP information that is not derived from certain [redacted] collections. It then refers to the retention rules[redacted] for USP information derived from certain [redacted] collections. [redacted] protect USP by requiring that the CIA only retain certain categories of USP information.[169]

---

164 (U//FOUO) CIA and PCLOB discussion, 8/24/16; CIA and PCLOB discussion, 8/18/16; CIA and PCLOB discussion, 7/6/16.

165 [redacted] CIA and PCLOB discussion, 11/4/15.

166 [redacted]

167 [redacted] also has policies regarding the handling of certain specialized types of information. Those policies are beyond the scope of this review. [redacted]

168 (U) Annex A §§ I.III, I.VI.; *see also* AR 2-2 § I.A(4)(b).

169 [redacted] For U.S. person information derived [redacted] other than the [redacted] collections covered [redacted] requires not only "strict accordance" with [redacted] more general retention rules, but also accordance with any special AG-approved minimization procedures, and "careful[] segregation." [redacted]

[redacted]

[redacted]

[redacted]Annex A's categories reflect a variety of factors that may support a decision to retain information. Some reflect processing techniques. For instance, the deletion of the identity of a USP and personally identifiable information may permit the retention of some information. Other categories reflect aspects of the collection's sourcing. For instance, information may be retained because it is "publicly available" or "consensual." Still other categories reflect the topic or value of the information to the agency. For instance, the agency can retain information that constitutes foreign intelligence. Additionally, Annex A permits retention for the sake of evaluation. In other words, Annex A permits retention when it "is necessary for a reasonable period to determine whether the information falls within one of the [other retention categories listed in Annex A]."[170]

[redacted] Among the Annex A retention categories, some correspond in obvious ways with those listed in Section 2.3 of E.O. 12333. But other Annex A categories use language distinct from that used in E.O. 12333 and thus do not correspond with the Section 2.3 categories in obvious ways. [redacted][171] some categories related to processing (*e.g.,* "information . . . processed to delete the identity of the U.S. person and all personally identifiable information"), and one category allowing retention for the sake of evaluation.[172]

[redacted]Annex A also supplements E.O. 12333 by incorporating a definition of "retention" that is set out in Appendix A. That definition is difficult to reconcile with Annex A's retention provisions, however. The Appendix A definition is "that information is organized in such a manner that it may be retrieved by reference to the name or identity of the person who is the subject of the information."[173] This definition is at odds with the context in which the word is used in Annex A. Specifically, Annex A permits USP information to be "retained" if it "cannot be retrieved by reference to the [U.S.] person's name or other identifying data."[174] In other words, Annex A expressly permits retention of information that does *not* satisfy the Appendix A definition of "retention."

[redacted] by contrast, requires additional measures to protect USP information [redacted] For retention and dissemination just within the CIA, [redacted] can be read to require deletion of a USP's identity and "all personally identifiable information" unless "the identity is necessary, or it is reasonably believed that it may become

---

[redacted] The Board assumes these techniques are a very small part, if any, of the covered activities. [redacted] not expressly addressed the techniques in its discussions with the Board.

170 (U) Annex A § I.VI.A.1.

171 [redacted]

172 (U) Annex A § I.VI.A.1.

173 (U) Annex G, Appendix A.

174 (U) Annex A § I.VI.A.1.d.

[redacted]

[redacted]

necessary, to understand or assess the information [about a USP]." If the latter scenario arises, [redacted] permits retention of a USP's identity only if the information also falls into one of [redacted] retention categories. The categories are similar to, but slightly different from, those in Annex A.

[redacted] does not contain language identical to Annex A's explicit statement in subsection (i) that information may be retained "for a reasonable period to determine whether the information falls within" one of the other permitted categories of retention.[175] Instead, [redacted] contains language that matches a different retention category [redacted]

[redacted]More specifically, Annex A includes subsection (VI)(A)(f)(4), a retention category that permits the CIA to retain information for the purpose of oversight or legal process obligations, including information that is "*necessary to be retained for the purpose of determining that the requirements of these procedures are satisfied*."[176] [redacted] contains nearly identical language, providing that: "Nothing [redacted] shall prohibit . . . the retention or disclosure of information *necessary for the purpose of determining whether the requirements of these procedures are satisfied . . . .*"[177]

[redacted] The CIA interprets the text of this provision [redacted] to permit retention for the purpose of evaluation.[178] However, since this language [redacted] matches subsection (f) of Annex A, an alternative reading would suggest that it does not also match subsection (i) of Annex A, the subsection that explicitly permits retention for evaluation.

[redacted]

175 [redacted] *See* Annex A, VI.A.1.i ("Such retention that is necessary . . . to determine whether the information falls within one of the categories above.")

176 *See* Annex A, VI.A.1 f.(4) (emphasis added).

177 [redacted]

178 (U//FOUO) CIA and PCLOB discussion, 11/22/16.

179 (U//FOUO) CIA and PCLOB discussion, 8/18/16.

180 (U//FOUO) CIA and PCLOB discussion, 8/18/16; *see* Annex A § I.VI.A.1.e., i.

[redacted]

[redacted]

[redacted]There is some tension between the alternative grounds for retention that attorneys cited, however. One ground, based on the provision allowing retention for evaluation, limits retention to a "reasonable period"; the other ground suggests no such time limit.[181] Additionally, none of the grounds for retention [redacted] cited draws on [redacted] determines whether its unstructured and structured data sets contain [redacted] information by reviewing the source of the information.[182] [redacted]

[redacted] stated that in practice, [redacted] Policy principally guides the group's retention practices. [redacted]

[redacted] Policy's retention rules rest on a framework that expands upon, and is different from, the framework established in Annex A. While Annex A defines types of information that can be retained, [redacted] Policy's protections turn on the concepts of "minimization" and "segregation," two methods of protecting USP information. As described by [redacted] E.O. 12333 collections of structured and unstructured financial data generally qualify for both.[185] The policy defines "minimize" as "the processing of information acquired by the Agency in order to permanently delete identifying U.S. person information that the CIA is not authorized to retain pursuant to Executive Order 12333 and HR 7-1 [now AR 2-2]."[186]

[redacted] Policy allows data that has been reviewed and "minimized" to be permanently retained.[187] But, it takes a different approach to unminimized data. The policy requires that for sets of aggregate data "that exceed the CIA's capacity to immediately review and minimize the information in its entirety upon receipt," segregated databases must be used to store the information until it is reviewed and minimized or deleted.[188] Information in those segregated databases must [redacted] understand as an interpretation of the "reasonable

---

181 (U//FOUO) *Compare* Annex A § I.VI.A.1.i *with* Annex A § I.VI.A.1.e.

182 [redacted] CIA and PCLOB discussion, 8/18/16. [redacted] CIA, *CIA Accuracy Review of PCLOB notes,* Statement 112 (May 10, 2016); CIA and PCLOB discussion, 4/21/15.

183 (U//FOUO) CIA and PCLOB discussion, 8/18/16.

184 [redacted] CIA and PCLOB discussion, 8/24/16; CIA and PCLOB discussion, 8/18/16; CIA and PCLOB discussion, 7/6/16; [redacted]

185 (U//FOUO) CIA and PCLOB discussion, 8/18/16; CIA and PCLOB discussion, 7/6/16.

186 [redacted]

187 [redacted]

188 [redacted]

189 [redacted]

[redacted]

[redacted]

period" that Annex A allows for information to be retained for evaluation.[190] Finally, the [redacted] Policy requires deletion of information "determined to be inappropriate for retention."[191]

[redacted] suggested that some collections of unstructured data may be small enough that they can be reviewed quickly,[192] [redacted] did not suggest it identifies and separates any structured or unstructured collections that can be reviewed immediately and minimized in their entirety upon receipt.[193]

[redacted], CIA does not consistently utilize the policy's definition of "minimization," a definition which CIA recognizes does not capture the full range of safeguards that may be applied to collected information. Instead of using [redacted] Policy's definition in applying the policy itself, [redacted] interprets "minimization" to include the masking, deletion, or segregation of USP information—as well as a determination that such information constitutes foreign intelligence.[194] [redacted]

[redacted] archiving requirement and retention limits to apply to data [redacted] The Policy went into effect [redacted]

190 (U//FOUO) CIA and PCLOB discussion, 8/18/16.
191 [redacted]
192 (U//FOUO) CIA and PCLOB discussion, 8/18/16; CIA and PCLOB discussion, 7/6/16.
193 [redacted]
194 [redacted] CIA and PCLOB discussion, 8/18/16; [redacted]
195 (U//FOUO) CIA and PCLOB discussion, 11/17/15.
196 (U//FOUO) CIA and PCLOB discussion, 8/18/16
197 [redacted]

[redacted]

[redacted]

[redacted]

[redacted] With regard to the retention limits on USP information [redacted] briefers consider [redacted] sets to be minimized through masking of USP information. Additionally, [redacted] sets are not segregated under the [redacted] Policy.[199]

[redacted] applies [redacted] Policy's deletion requirement rarely, if at all. [redacted] CIA officials explained that in financial data, there is not a type of data that would routinely be considered inappropriate for retention on first review; rather, any information that is unimportant to one exploiter might be valuable to another, upon later review. In this regard, briefers contrast financial data to other types of information, [redacted] that might have categories of information [redacted] that are deemed inappropriate for retention immediately.[200]

[redacted] For this and other reasons, [redacted] no regular practice of deleting either the structured data [redacted] or unstructured data. When one [redacted] system or tool retrieves [redacted] E.O. 12333 financial records, the system maintains the information for other users who may find it useful. Any information a user deems appropriate for an intelligence report or other analysis is copied, retained, and/or disseminated separately.[201] Furthermore, as explained above, [redacted] not yet applied [redacted] Policy's (or any other) requirement to archive or delete information due to its age. [redacted] retains backup copies of its data sets. [redacted]

[redacted] applies in cases in which the IC element has not yet affirmatively determined what retention period would apply to such information, if it concerned USPs, under the element's AG-approved procedures implementing Section 2.3 of E.O. 12333. In other words, with certain exceptions, [redacted]

198 [redacted] CIA and PCLOB discussion, 8/18/16.
199 (U//FOUO) CIA and PCLOB discussion, 7/6/16; CIA and PCLOB discussion, 8/18/16.
200 (U//FOUO) CIA and PCLOB discussion, 8/18/16.
201 (U//FOUO) CIA and PCLOB discussion, 8/18/16; CIA and PCLOB discussion, 11/4/15.
202 (U//FOUO) CIA and PCLOB discussion, 7/6/16; CIA and PCLOB discussion, 11/4/16.

[redacted]

and is "unevaluated."[203] procedures apply this cap to personal information regarding non-USPs and direct that AR 2-2 governs the retention of personal information regarding USPs.[204]

Across the agency, the CIA has not yet reached final determinations regarding which individual collections should be made subject Thus, at the time of the Board's review, it was unclear how CIA's implementing rules and guidance would change the group's retention practices.[207] The agency aims to have the necessary procedures for implementing these requirements in place Pending a collection-by-collection determination, limit to all of the data sets available as the CIA has concluded that at least some fall within the scope

As with regard to collection, methods for complying with applicable rules focus on operating practices, not after-the-fact compliance reviews. In examining the extent to which complied with applicable rules, the CIA OIG found did not periodically review the system for compliance

203

204

205

206

207 (U//FOUO) CIA and PCLOB discussion, 8/18/16, 11/8/16.

208 (U//FOUO) CIA and PCLOB discussion, 8/18/16; CIA and PCLOB discussion, 7/6/16.

209

[redacted]

[redacted] The CIA OIG also found that this practice was consistent with the treatment of other [redacted] systems.[210]

4. (U//FOUO) New AG-approved procedures

[redacted]The New Procedures supplant [redacted] as well as Annex A's more general rules.[211] As noted above, the New Procedures expressly apply to incidentally collected USP information. Furthermore, [redacted]the New Procedures (1) directly address the handling of unevaluated information, *i.e.*, information that has not been determined to qualify for indefinite storage, and (2) establish clear time limits on the CIA's storage of certain types of information. [redacted]

[redacted]The New Procedures' retention framework rests on a new definition of retention: the "indefinite maintenance of information concerning U.S. persons," subject to certain exceptions.[213] The procedures include one set of rules for "retention," as defined in the procedures, and a separate set of rules for the temporary "storage" of unevaluated information, *i.e.*, "information that has been collected but not yet reviewed to determine whether it relates to an authority or responsibility [of the CIA] and whether information concerning U.S. persons, if any, qualifies for retention."[214]

[redacted]Similarly to the[redacted] Policy, the New Procedures set time limits on the CIA's storage of certain unevaluated information. The New Procedures' framework does not, however, match[redacted] current practice or [redacted] Policy's requirements exactly. Instead, the New Procedures create two tiers of handling requirements for unevaluated information. Each tier has a separate limit on how long the CIA can store data in the relevant category, and allows the retention period to be extended in certain circumstances. The shortest storage period, five years, applies to information subject to "exceptional handling requirements," which falls into two categories: (2) certain non-consensual, non-public communications [redacted] and (2) "[u]nevaluated information that, due to special circumstances, is anticipated to contain USPII [USP identifying information] that is substantial in volume, proportion, or sensitivity."

[redacted]In addition to being deleted after five years, these two categories of information must be segregated from other categories of information.[215] The longer storage period, 25 years, applies

---

210 (U) OIG Report[redacted]

211 (U//FOUO) CIA and PCLOB discussion, 8/24/16.

212 ([redacted]

213 (U//FOUO) New Procedures § 12.21 (emphases omitted).

214 (U//FOUO) New Procedures § 12.22 (emphases omitted); *see* New Procedures §§ 6, 7.

215 [redacted]New Procedures § 6.2.2. The New Procedures define USP identifying information, or U.S. person identifying information, as "information that is reasonably likely to identify one or more specific U.S. persons" and

[redacted]

[redacted]

to information subject to "routine handling procedures," which is all information not subject to exceptional handling requirements.[216] The longer storage period also applies to unevaluated information (except for nonpublic communications) that is otherwise subject to exceptional handling requirements when USP identifying information has been masked or obfuscated. [217]

[redacted]Separately, the New Procedures set forth a framework for the indefinite storage, *i.e.*, "retention," of other information. In general, they allow the CIA to indefinitely retain information concerning USPs that has been "evaluated and determined to meet the criteria" listed in the procedures.[218] This framework is similar to[redacted] officials describe as their current practice for information that constitutes foreign intelligence, but the New Procedures' reference to indefinite storage is more explicit [redacted] with regard to the *length* of permissible retention.

[redacted]Similarly to Annex A, the New Procedures also include grounds for retention that do not expressly match the categories of USP information listed in Section 2.3 of E.O. 12333.[219] But, the criteria listed for "retention" under the New Procedures reflect some differences from the grounds for retention listed in Annex A [redacted] in part because unevaluated information is treated as "stored" rather than "retained." For instance, in light of their separate handling of unevaluated information, the New Procedures do not contemplate "retention" for a "reasonable period" to evaluate whether other retention grounds apply. The New Procedures also omit Annex A's allowance for the CIA to retain USP information on the basis of how identifying information is handled. In other words, unlike Annex A, the New Procedures do not allow permanent retention of information indefinitely merely because it is (1) identifying, or (2) stored such that it cannot be retrieved by reference to identifying data.[220]

C. [redacted]Exploiting and sharing E.O. 12333 financial information

[redacted]After processing (and to some extent during processing),[redacted] makes its E.O. 12333 financial data available for exploitation within the CIA and sharing outside the agency. [redacted] describes two goals for its use and sharing of financial information regarding ISIL: (1) informing policymakers, *e.g.*, by providing insight into ISIL's financial operations, and (2) enabling action, such as arrests, by other entities.[221]

---

note that it is a "subset of information concerning a U.S. person." New Procedures § 12.25.

216 (U//FOUO) New Procedures § 6.3.1, 6.3.3.2.

217 (U//FOUO) New Procedures § 6.3.1(b), 6.3.2.

218 (U//FOUO) New Procedures § 7.

219 [redacted] For example, the New Procedures expressly permit retention of information that is processed to delete USP "identifying information," but not all USP information. They also permit retention of information "suspected to be enciphered." *Compare* New Procedures § 7 *with* Exec. Order 12333 § 2.3.

220 (U//FOUO) *Compare* New Procedures § 7 *with* Annex A § I.VI.A.1.a, d, i.

221 [redacted]

[redacted]

[redacted] has two primary modes for using and sharing financial information that can be used vis-à-vis ISIL. First, [redacted] shares structured information that is unevaluated. Second, [redacted] produces and distributes intelligence products, *i.e.*, information that has been evaluated and has been deemed to constitute foreign intelligence or counterintelligence. [redacted] intelligence reports capture the results of [redacted] exploitation of its financial data. The group performs what it terms "first order" analysis: analysis of the group's E.O. 12333 financial data holdings, sometimes in combination with other financial data and/or non-financial data [redacted][2]

[redacted] use and sharing of information regarding ISIL complements other CIA components' efforts. As discussed above, the Counterterrorism Mission Center [redacted] distribute finished intelligence: products that reflect all-source analysis.[223] Field stations collecting information may also document information directly into narrative foreign intelligence.[224]

[redacted] Section 1 below discusses the practice for sharing and using E.O. 12333 financial data within the CIA. Section 2 regards the sharing of such data outside the CIA. Sections 3 through 5 discuss various sets of applicable rules and Section 7 discusses the New Procedures.

1. [redacted] The use and sharing of unevaluated E.O. 12333 financial data within the CIA

a) [redacted] Structured financial data

[redacted] allows personnel [redacted] and other CIA components access to [redacted] unevaluated structured data sets [redacted]

[redacted] CIA has made [redacted] available to users after receiving a request describing the individual's job function, justification, and supervisor's name and

---

222 [redacted] CIA and PCLOB discussion, 8/24/16; CIA and PCLOB discussion, 7/6/16; CIA and PCLOB discussion, CIA and PCLOB discussion, 11/4/15; CIA and PCLOB discussion, 9/21/15; CIA and PCLOB discussion, 8/7/15.

223 [redacted] CIA and PCLOB discussion, 7/6/16; CIA and PCLOB discussion, 11/4/15; (9.10) [redacted]

224 (U//FOUO) CIA and PCLOB discussion, 8/24/16.

225 (U//FOUO) CIA and PCLOB discussion, 7/6/16; CIA and PCLOB discussion, 11/16/16.

[redacted]

contact information.[226] The CIA is currently making changes in the access protocols in response to recommendations from the CIA OIG.[227]

With capabilities that allows users to analyze information across numerous data sets, in a variety of ways. Users can perform keyword and more advanced types of searches Other tools map linking groups of individuals or entities against a timeline. Users can also view profiles of individuals or other entities. consolidates portfolios of records that the tool has identified as belonging to the same person.[228]

officials describe a single standard for CIA searches, regardless of whether those searches involve information related to USPs or information related to other persons: the query must have a foreign intelligence or operational purpose.[229] In general, training and reference materials alert users that they can start with broad searches and then narrow down results to reach key information.[230] A feature allows "bulk" searches, *i.e.*, searches using multiple selectors simultaneously.[231] representatives suggested that one type of search this feature could facilitate would be to run a list of individuals through the new data set, such as a list of individuals associated with a particular terrorist group

With these allowances for broad searches, however, includes two key protections for information concerning USPs. First, the tool limits the results provided when

---

226 CIA and PCLOB discussion, 8/18/16;

227 CIA and PCLOB discussion, 7/6/16; CIA and PCLOB discussion, 11/16/15.

228 CIA and PCLOB discussion, 8/18/16; CIA and PCLOB discussion, 11/16/15. In creating profiles of particular entities, the system includes measures to reduce the risk of mistaken identities. To consolidate records, it requires that spelling matches be exact that and records that share both a name and another attribute. CIA and PCLOB discussion, 11/16/15.

229 (U//FOUO) CIA and PCLOB discussion, 8/18/16; CIA and PCLOB discussion, 7/6/16.

230 "We felt it was best to allow you to search without the need to narrow the data to be searched. So go ahead and search If you get too many results, then you can narrow your search . . . ."

231

232 (U//FOUO) CIA and PCLOB discussion, 8/24/16;

[redacted]

users base their queries on USP information. As described above, [redacted] runs the [redacted] algorithm to automatically identify and then mask certain personally identifiable information regarding assumed USPs. If CIA personnel search [redacted] using the name of an identified USP, the results may be returned with that USP's name and other identifying information redacted.[233]

[redacted] rules include a protection for USP information that [redacted] cannot identify on an automated basis. [redacted] reference materials, including the splash screen that appears each time a user accesses the site, instruct users to nominate for review any data they come across that they suspect regards a USP. The nominated record is masked if it is determined to constitute USP information. Unlike the masking process, however, the nomination process is not automatic and depends on users complying with their obligation to identify USP information. [redacted] the electronic button for nominating information is more prominent than it was [redacted] But the instruction to users about their obligation to nominate comes in the form of a small-print computer screen notice that includes a number of other points.[234]

[redacted] Even with these protections, [redacted] limitations on the retrieval and review of USP identifying information are not absolute. [redacted] users who wish to retrieve masked information regarding USPs can submit requests accompanied by "[a] written certification from the requester's management that the unmasked request is authorized activity by the requester and that the identifying information is necessary to understand the foreign intelligence," as well as "[a] detailed explanation as to what purpose the information is needed for and whether [the requester] would like to share this information outside of [the requester's] agency." Approval by the requester's supervisor as well as CIA legal staff concurrence is necessary.[235] [redacted] the requester's supervisor reviews the justification and the attorney reviews the request for compliance with the procedure.[236] Any released data goes only to the requester, with a warning to follow the procedures of the requester's agency regarding the handling of USP information.[237] [redacted] attorney's rough estimate was [redacted] receives [redacted] unmasking requests in a year.[238]

---

233 (U//FOUO) CIA and PCLOB discussion, 8/18/16; CIA and PCLOB discussion, 11/4/15; *see supra* p. 33.

234 [redacted] CIA and PCLOB discussion, 11/16/15.

235 [redacted]

236 [redacted] CIA and PCLOB discussion, 7/6/16. [redacted] reporting team also reviews the request to determine whether release would be consistent with the protection of sources and methods. *Id.*

237 (U//FOUO) CIA and PCLOB discussion, 9/21/15; *see also* CIA and PCLOB discussion, 11/4/15.

238 (U//FOUO) CIA and PCLOB discussion, 7/6/16.

[redacted]

[redacted]

b) [redacted] Unstructured financial data

[redacted] team may query the unstructured E.O. 12333 data it holds as frequently as it queries structured data.[239] [redacted] takes a more limited approach to sharing that information. [redacted] does share unevaluated unstructured information [redacted] Furthermore, [redacted] has recently begun to limit access to unstructured data to a small number of subject matter experts, who review the information [redacted] depending on where it is stored.[240]

[redacted] these experts can use a tool [redacted] that facilitates limited key word searches. [redacted] can be used for basic searches. But [redacted] review often means document-by-document review and translation, as necessary. [redacted] do not have methods for conducting sophisticated searches across multiple collections.[241]

[redacted] In reviewing information [redacted] any reviewer may come across USP information [redacted] unstructured, it cannot be processed using automated masking tools [redacted] protect USP information through access limitations, though the CIA OIG identified weaknesses in those limitations.[243] Also, [redacted] officials stated that [redacted] rules protect USP information by requiring users to nominate for masking any USP information that they find and identify as such.[244] It is not clear, however, where such requirements are documented. The CIA represented that there are no user manuals or similar documents [redacted] do not reflect this requirement, and the CIA did not produce any such documents [redacted]

[redacted] user agreements for unstructured data represent a different type of protection for USP information. Among other things, they remind users that access is only permitted to identify information of foreign intelligence or counterintelligence value.[246] [redacted]

---

239 (U//FOUO) CIA and PCLOB discussion, 11/16/15.

240 [redacted] CIA and PCLOB discussion, 8/18/16; CIA and PCLOB discussion, 7/6/16; CIA and PCLOB discussion, 9/21/15.

241 [redacted] CIA and PCLOB discussion, 7/6/16; CIA and PCLOB discussion, 11/16/15; CIA and PCLOB discussion, 11/4/15; E-mail from Office of Privacy and Civil Liberties, CIA, to PCLOB staff (May 25, 2015).

242 (U) *See generally* CIA and PCLOB discussion, 8/24/16.

243 (U) OIG Report [redacted] CIA and PCLOB discussion, 8/24/16.

244 (U//FOUO) CIA and PCLOB discussion, 8/24/16.

245 [redacted] E-mail from Office of Privacy and Civil Liberties, CIA, to PCLOB staff (May 25, 2015) [redacted] E-mail from Office of Privacy and Civil Liberties, CIA, to PCLOB staff (May 23, 2015) [redacted]

246 [redacted]

[redacted]

[redacted]

[redacted] The data sets represented a new level [redacted] so the group looked to some of its procedures related to programs [redacted] and drafted the agreements to ensure that both users and their managers were reminded of existing requirements.[247]

2. [redacted] The sharing of E.O. 12333 financial data outside the CIA

a) [redacted] Sharing of unevaluated structured information

[redacted] shares unevaluated structured information outside the CIA [redacted] The external audience consists of other federal agencies. [redacted]

[redacted]

247 (U//FOUO) CIA and PCLOB discussion, 8/18/16; CIA and PCLOB discussion, 7/6/16; CIA and PCLOB discussion, 6/13/16.

248 [redacted] CIA and PCLOB discussion, 8/18/16; CIA and PCLOB discussion, 11/4/15. [redacted] CIA and PCLOB discussion, 7/6/16.

249 E-mail from Benjamin Huebner, Privacy and Civil Liberties Officer, CIA, to PCLOB staff (Sept. 16, 2016); [redacted]

250 (U//FOUO) CIA and PCLOB discussion, 8/18/16.

251 (U//FOUO) CIA and PCLOB discussion, 8/24/16; CIA and PCLOB discussion, 11/16/15.

[redacted]

[redacted]

b) [redacted] Sharing of evaluated information[257]

[redacted] analysts disseminate the results of their "first order analysis" [redacted] through several types of intelligence products. Internally through cables [redacted] provides information to others within the CIA. For external distributions, [redacted] narrative foreign intelligence reports, or "telegraphic disseminations" ("TDs"), and Central Intelligence Reports ("CIRs"), two types of reports that are not considered "finished" intelligence because although they contain information believed to be credible, they have not received a formal CIA assessment that they are correct.[259] TDs contain information that meets a standard abbreviated as FINCA: foreign, of interest, new, clandestine, and authoritative.[260] TDs

---

252 [redacted] CIA and PCLOB discussion 7/6/16; CIA and PCLOB discussion, 12/16/15; CIA and PCLOB discussion, 11/4/15. The CIA OIG reviewed the procedures for nominating data for release [redacted] The CIA OIG conclude that the procedures "were effective in ensuring that only minimized bulk financial data are disseminated." The CIA OIG also "confirmed that USP information masked on the [redacted] is also masked on the [redacted] OIG Report [redacted].

253 [redacted] CIA and PCLOB discussion, 8/18/16; [redacted]

254 [redacted] E-mail from Office of Privacy and Civil Liberties, CIA, to PCLOB staff (May 25, 2015).

255 (U//FOUO) CIA and PCLOB discussion, 8/24/16.

256 [redacted].

257 (U) In this report, the term "evaluated" refers to information that has been reviewed and deemed to meet CIA requirements for permanent or indefinite retention. If, however, the report refers to a document that includes a definition of "evaluated," that document's definition applies.

258 [redacted]

259 (U//FOUO) CIA and PCLOB discussion, 8/18/16; CIA and PCLOB discussion, 11/4/15.

260 (U//FOUO) CIA and PCLOB discussion, 11/4/15.

[redacted]

[redacted]

document what CIA considers narrative foreign intelligence;[261] they are required to be tied to a NIPF topic.[262] TDs are sent to higher-level audiences within the IC and can also be sent to foreign governments.[263] CIRs, by contrast, are used to share information that is deemed of intelligence value but is not complete enough to meet the FINCA standard.[264] [redacted] also use CIRs to document communications with other agencies that may be for other purposes. [redacted]

[redacted] For each type of intelligence product that CIA distributes, there are requirements that may include protections for USP information. Those requirements cover the product's contents, as well as documentation that should be included in a separate accompanying cable [redacted]

3. [redacted] Key rules [redacted] implementation: Data usage

[redacted] E.O. 12333, Annex A, and [redacted] Policy provide limited guidance for [redacted] use of financial data. All three documents direct generally that CIA activities must fit within authorized boundaries.[268] In implementing the requirements of E.O. 12333 and AR 2-2, the [redacted] Policy provides additional instruction regarding the CIA's use of unminimized data in segregated databases. The policy directs that access should be limited to "CIA personnel with a legitimate need to access the data in order to conduct minimization." It further recommends masking algorithms and other technologies to minimize access to personally identifiable information, while recognizing the need to balance use of technologies against access needs. Furthermore, the policy requires "[t]o the extent practicable . . . an auditable record of user activity within segregated databases, to include a record of data accessed by each user."[269]

---

261 [redacted]

262 (U//FOUO) CIA and PCLOB discussion, 11/4/15.

263 (U//FOUO) CIA and PCLOB discussion, 8/18/16; CIA and PCLOB discussion, 11/4/15; CIA and PCLOB discussion, 5/4/16.

264 (U//FOUO) CIA and PCLOB discussion, 11/4/15.

265 (U//FOUO) CIA and PCLOB discussion, 8/18/16; CIA and PCLOB discussion, 11/4/15.

266 (U//FOUO) CIA and PCLOB discussion, 8/18/16.

267 [redacted]

268 (U//FOUO) E.O. 12333 § 2.3 (referencing part 1 of the order); Annex A § I.III; [redacted]

269 [redacted]

[redacted]

[redacted] rely more on access limitations than on masking and audit capabilities. As described above, because these are unstructured databases, the CIA cannot rely on automated tools in this context and therefore USP information can only be masked in response to a specific request from a user. Furthermore, [redacted] did not have an auditing mechanism. Instead of monitoring use [redacted] focused on limiting access and monitoring the list of people with access to make sure that it was still needed.[271]

[redacted] has also not routinely audited [redacted] to enforce its protections for USP information. Though [redacted] allowed some monitoring or auditing of usage, [redacted] users are warned of such monitoring, [redacted] generally only performed audits to address particular cases of concern.[272]

[redacted] is in the process of enhancing its monitoring and auditing practices, however. [redacted] built with more advanced auditing capabilities [redacted] and the group is increasing its monitoring of usage. Though the increased monitoring has initially focused on security and safety concerns, [redacted] representatives explain three reasons why they will begin to more routinely and directly audit usage. The first regards the changes in retention rules [redacted] the New Procedures may require. As explained above, to the extent that any of these rules apply [redacted] seeks to be prepared to develop data-driven requests for extended retention periods for collections that are providing value. Second, the New Procedures include requirements regarding the auditability of unevaluated information, and also require auditing of information systems, though the latter requirement focuses on auditing by oversight entities [redacted] The third reason is that [redacted] receiving requests to broaden access within the CIA to its data and tools. [redacted] concluded that while limiting access has earlier been sufficient to ensure compliance with key rules, broader access requires broader auditing.[274]

---

270 [redacted]

271 [redacted] CIA and PCLOB discussion, 8/18/16; CIA and PCLOB discussion, 7/6/16. Furthermore, though access controls are generally outside the scope of this review, the Board notes that the CIA OIG concluded that as [redacted] were not strict enough. OIG Report [redacted] As of March 2016, measures to address the CIA OIG's concerns were in progress. OFFICE OF INSPECTOR GEN., CIA, [redacted]

272 [redacted] CIA and PCLOB discussion, 8/18/16; CIA and PCLOB discussion, 7/6/16.

273 (U//FOUO) New Procedures §§ 6.2.2.1, 6.3.3.1, 10.1.

274 (U//FOUO) CIA and PCLOB discussion, 8/18/16; CIA and PCLOB discussion, 7/6/16.

[redacted]

4. [redacted] Key rules [redacted] implementation: Sharing information [redacted]

[redacted] Like other aspects of its E.O. 12333 activities, [redacted] sharing of financial data is governed by E.O. 12333, Annex A, [redacted] Policy. Other [redacted] policies set forth additional interpretations and requirements.

[redacted] E.O. 12333's framework for the dissemination of USP information is similar to its framework for the collection and retention of such information. The same Section 2.3 list of types of USP information applies. Section 2.3 also provides that an IC element may disseminate information to another IC element for that element "to determine whether the information is relevant to its responsibilities and can be retained by it." [redacted]

[redacted] Annex A uses a framework for dissemination that is similar to its framework for retention. The document sets out dissemination rules for US person information that is not derived from [redacted] It then refers to the dissemination rules [redacted] for US person information derived from [redacted]

[redacted] In general, Annex A repeats E.O. 12333's provision for dissemination of information to other IC elements to determine whether the information can be retained by them. For other disseminations of USP information outside the agency, Annex A protects USP information by requiring that the information satisfy both the Annex's retention requirements and additional requirements specific to particular sets of recipients. For instance, executive agencies must "need the information to perform their lawful function." Annex A's dissemination rules also address sharing of information within the CIA; it requires "a need to know."[277]

[redacted] For the *identity* of a USP, however, Annex A imposes a special protection, as discussed above. Such information can be disseminated with other information about the person only "if the information qualifies for retention and dissemination [under Annex A's general retention and dissemination provisions] and if the identity is necessary or if it is reasonably believed it may become necessary to understand or assess such information."[278] [redacted]

---

275 [redacted]

276 (U) Annex A § I.VI.A.2 [redacted]

277 (U) Annex A § I.VI.A.2.

278 (U) Annex A § I.VI.A.3. Annex A does not expressly state whether this special restriction applies to some or all disseminations.

[redacted]

[redacted]

With regard to disseminated bulk data, [redacted] policy concludes that the "CIA must take reasonable steps to ensure that disseminated bulk data does not include identifiable information on U.S. persons unless such information is necessary for understanding the FI [foreign intelligence]/CI [counterintelligence] value of the data."[280]

[redacted] sets out a similar, but different, set of protections for USP information [redacted] As discussed above in the context of retention,[281] [redacted] requires deletion of the identity of a USP "and all personally identifiable information" for disseminations except if two requirements are satisfied. The first requirement is Annex A's statement that the USP information must be "necessary or reasonably believed that it may become necessary" to understand the value of the data. The second is that the accompanying information must fall into one of several listed categories, *i.e.* that the information constitutes foreign intelligence or counterintelligence or meets one of the other listed categories for retention. The listed categories are similar to, but not exactly the same as, Annex A's retention categories. As a result, [redacted] requirements regarding USP identifying information operate similarly to Annex A's, though each document presents the applicable requirements in a distinct manner.[282]

[redacted] Like the rules regarding retention, [redacted] on their face, include several potential ambiguities. [redacted] leave some uncertainty as to whether they limit the dissemination of USPs' identities *within* the CIA, as well as with regard to disseminations *outside* the CIA. Furthermore, Annex A can be read to allow the broad dissemination of information being retained only for review—an allowance that seems at odds with Annex A's general framework for protecting USP information. A CIA training developed in 2015 addresses at least the first point; it suggests that the "necessary to understand" limitation on the sharing of USPs' identities does not apply within the CIA—and may only apply to the sharing of information *outside* the IC.[283]

[redacted] representative explained [redacted] considers its practices for disseminating unevaluated financial data to satisfy the strictest AR 2-2 dissemination standards, *i.e.*, the [redacted] standards regarding [redacted] through the masking of USP identifying information [redacted] The Board notes [redacted] standard for unmasking

279 [redacted]

280 [redacted]

281 [redacted]

282 [redacted]

283 [redacted] CIA and PCLOB discussion 10/29/15 (regarding launch of training).

284 (U//FOUO) CIA and PCLOB discussion, 8/18/16; CIA and PCLOB discussion, 7/6/16.

[redacted]

[redacted]

USP identifying information [redacted] is very similar to the "necessary to understand" standard in Annex A [redacted]

[redacted] explained controls on disseminations of evaluated intelligence that includes USP information. [redacted] officers are responsible for determining whether any such dissemination of USP identifying information satisfies the "necessary to understand" standard. Then, attorneys review the products before they are disseminated and ask for an explanation of any non-minimized USP information.[286] [redacted] representatives did not address the additional requirements [redacted] the Board notes that in the context of covered activities, the sharing of *evaluated* information regarding ISIL should satisfy one of the options [redacted] for dissemination: it will constitute either foreign intelligence or counterintelligence.[287]

[redacted] In this area, as in others, [redacted] representatives emphasized their use of the [redacted] Policy, as well as other policies regarding dissemination.[288] Both the [redacted] Policy and other polices that the CIA provided or summarized for the Board include substantive or procedural limits on certain disseminations. At a high-level, they require special attention to disseminations of not only USP identifying information [redacted] applicable policies require analysis of the potential harm to those USPs and approval from senior

[redacted]

285 [redacted]

286 (U//FOUO) CIA and PCLOB discussion, 8/24/16.

287 (U) *See* E.O. 12333 § 3.5(a) and (e) (defining "foreign intelligence" to encompass information regarding "international terrorists" and "counterintelligence" to encompass information regarding "international terrorist organizations or activities").

288 (U//FOUO) CIA and PCLOB discussion, 8/18/16; CIA and PCLOB discussion, 7/6/16.

289 [redacted]

[redacted]

[redacted]

officials. In general, the policies require higher level of approvals when more serious harm may be expected, though exceptions are permitted for disseminations [redacted] for counterterrorism purposes.[290] A [redacted] policy also requires that when USP information is disseminated [redacted] in response to a request, that the dissemination is limited to the information "specifically requested [redacted]

[redacted] Policy also includes more general dissemination standards for other types of aggregate data. Annex A provides a more granular list of options and requirements, and the [redacted] Policy states generally that recipients with a "need to know" can receive information that has been "reviewed and determined to constitute foreign intelligence (or otherwise minimized consistent with Executive Order 12333 and HR 7-1 [now AR 2-2])."[292] The [redacted] Policy—like Annex A—also limits the dissemination of unminimized data that has not been determined to constitute foreign intelligence, though the [redacted] Policy's limitation is primarily procedural; it requires [redacted] management approval.[293]

5. [redacted]

[redacted]

290 [redacted]

291 [redacted]

292 [redacted]

293 [redacted]

294 [redacted]

295 [redacted]

296 [redacted]

297 [redacted]

298 [redacted]

[redacted]

[redacted]

[redacted]

6. (U//FOUO) New AG-Approved Procedures

[redacted]The New Procedures address the distribution of information inside and outside the CIA and include several mechanisms for protecting USP information. As noted above, unlike Annex A [redacted] the New Procedures expressly address how the protections should apply to incidentally collected USP information, by setting out rules for unevaluated information and noting that "unevaluated information is generally presumed to contain incidentally acquired information concerning U.S. persons."[301]

[redacted]For providing information to CIA personnel, the New Procedures, like Annex A, focus on a need-to-know requirement.[302] The New Procedures also mention access limitations that Annex A does not discuss (though other CIA policies may). They require security clearance, access approval, and a mission requirement for access to information concerning USPs.

[redacted]The New Procedures also address CIA employees' queries of information, a subject that Annex A does not address expressly. For queries of retained information, the New Procedures require that queries, regardless of whether they involve USP information, be "reasonably designed to retrieve information related to a CIA authority and responsibility."[303] The New Procedures apply the same standard to queries of unevaluated information that is being held under the procedures' "routine" handling requirements.[304] But for unevaluated information subject to the New Procedures' "exceptional" handling requirements, the New Procedures would

---

[redacted]

299 [redacted] CIA and PCLOB discussion, 8/18/16; [redacted]

300 [redacted] CIA and PCLOB discussion, 8/9/16.

301 [redacted]New Procedures §§ 8 (regarding dissemination), 12.22 (defining "unevaluated information").

302 [redacted]*Compare* New Procedures § 8.1 *with* Annex A § I.VI.A.2.

303 (U//FOUO) New Procedures § 7.

304 (U//FOUO) New Procedures § 6.3.4.

[redacted]

[redacted]

set out additional limits on queries designed to retrieve information concerning a USP. For any such query of unevaluated information subject to exceptional handling requirements, either the USP must have consented or "to the extent practicable," the query must be "accompanied by a statement explaining the purpose of the query."[305]

[redacted]With regard to the provision of evaluated information outside the CIA, the New Procedures largely preserve the framework of Annex A, but reflect some changes in the permissible grounds for and audiences of such disseminations. Compared to the current Annex A, some of the changes appear to broaden the circumstances in which dissemination would be permitted (*e.g.*, by allowing dissemination to any audience of publicly available information), and others narrow such circumstances (*e.g.*, by requiring, in certain cases, documentation of risks and benefits that Annex A does not require).[306]

[redacted]The New Procedures expressly allow the dissemination of unevaluated information outside the IC, although they require that personnel first conduct a benefits and risk analysis and comply with other substantive and documentation standards.[307] Consistent with E.O. 12333 and like Annex A, the New Procedures also allow dissemination of USP information to IC elements for those elements to determine whether the information is relevant to their responsibilities and can be retained by them. [redacted] does not permit such disseminations of USP information [redacted] and thus the New Procedures are more permissive in this regard.[308]

[redacted] Finally, the New Procedures narrow the requirement for deleting USP identifying information in disseminated material. Most notably, the New Procedures require the removal of USP identifying information prior to dissemination only for dissemination outside the IC and, for those disseminations, only "[t]o the extent practicable," unless the USP identifying information is necessary to understand, assess, or act on the disseminated information. Annex A [redacted] a "necessary to understand" allowance, but do not include the "to the extent practicable" qualification. Further, [redacted] only allows "necessary to understand" disseminations under listed circumstances.

[redacted]Unlike Annex A, the New Procedures address audits as a means of enforcing protections for USP information. With some exceptions for practicability, the New Procedures generally require the CIA to maintain an auditable record of all activity concerning unevaluated

---

305 (U//FOUO) New Procedures § 6.2.3(b)-(c).

306 [redacted] *Compare* New Procedures § 8.2 *with* Annex A § I.VI.A.2; *compare also* New Procedures § 7 (grounds for retention that § 8.2 incorporates by reference) *with* Annex A § I.VI.A.1 (grounds for retention that § I.VI.A.2 incorporates by reference). The procedures also limit the term "dissemination" to distributions of information outside the CIA. New Procedures §§ 8.1, 13.8.

307 (U//FOUO) *Compare* New Procedures § 8.2.2 *with* Exec. Order § 2.3 *and* Annex A § I.VI.A.2 [redacted]

308 (U//FOUO) *Compare* New Procedures § 8.1 *with* Annex A § I.VI.A.2 [redacted]

[redacted]

information stored by the CIA. The record would include details about "access, queries made, and justifications for queries."[309] As noted above, the New Procedures further mandate that agency "information systems . . . be designed to facilitate auditing of access to and queries of information" and state that "these systems shall be audited by the appropriate oversight entities."[310]

[309] (U//FOUO) New Procedures §§ 6.2.2.1; 6.3.3.1.

[310] (U//FOUO) [redacted]. New Procedures § 10.1. The New Procedures list a variety of internal and external oversight entities that may have some role in oversight. *Id.* at § 10.2.

[redacted]

IV. (U) EVALUATION AND RECOMMENDATIONS

(U) This section analyzes the extent to which the covered activities and the policies they implement appropriately balance the need to protect the Nation from terrorism with the need to protect USPs' privacy and civil liberties. Balancing these priorities required the Board to take into account four key factors. First, USP information implicated by the covered activities is largely collected incidentally outside of the United States.

[redacted] Second, the ISIL threat is serious and it is both evolving and international in nature. Combatting this threat is a high priority for U.S. counterterrorism efforts, and it demands flexibility and creativity in the collection and use of financial intelligence.[311]

[redacted] Third, because some types of financial intelligence can be sensitive or revealing, [redacted] activities potentially impact the privacy of USPs whose information [redacted] has collected. As described above, these records and other parts of [redacted] E.O. 12333 data can include

[redacted]

(U) Based on these considerations, the discussion below examines potential risks to privacy and civil liberties and presents related recommendations regarding the covered activities and the policies that govern them. In each section, the Board first presents its analysis based on the

311 [redacted]
312
313
314
315

[redacted]

[redacted]

activities as they were conducted at the time of the Board's review: namely, under the AG Procedures adopted in 1982. Each section then proceeds to explore how PCLOB anticipates implementation of the new AG Procedures ("New Procedures") to address the risks identified.

A. (U//FOUO) Incidental collection of USP information abroad

The AG Procedures governing [redacted] collection of information do not explicitly address the incidental collection of USP information abroad when the CIA collects that USP information as an incident to collection in bulk or without a USP target. [redacted] mitigated this potential gap through the [redacted] Policy, which directs [redacted] to assume that bulk financial intelligence contains USP information and imposes a set of rules to safeguard that financial intelligence.

[redacted] Below, the Board considers the extent to which the [redacted] Policy, in conjunction with Annex A of the CIA's current Attorney General-approved procedures, safeguards privacy. The Board also describes the extent to which implementation of the New Procedures is likely to resolve any issues the Board has identified under the current AG-approved procedures.

1. (U//FOUO) Analysis based on existing policy

[redacted] The covered activities include collecting structured financial records [redacted] In many cases, these collections include information about [redacted] assumes that these collections contain USP information, even when [redacted] has not targeted specific USPs. [redacted] result in some incidental collection of USP information.

[redacted] Annex A's requirement [redacted] use the least intrusive category of techniques feasible applies only to collections occurring inside the United States or when the target is a USP. [redacted] directs its intelligence activities at non-USP targets abroad, including conducting bulk collection directed at identified [redacted], this requirement does not apply to collections covered by this report,[316] even though [redacted] expects to incidentally acquire USP information.

[redacted] The CIA has advised that, as a practical matter, personnel frequently use the least intrusive means feasible, for operational reasons. [redacted] has not represented that this is always the case, and there may be circumstances in the future [redacted] in which operational expedients and voluntary application of this safeguard are at odds.

316 [redacted] Annex A § I.IV.D.

[redacted]

[redacted]

[redacted] Policy, which imposes several privacy-enhancing safeguards related to data management,[317] also requires [redacted] personnel take "reasonable steps to limit the inadvertent collection of non-pertinent information that is of little or no intelligence value."[318] Illustrating one possible application of the "reasonable steps" requirement, [redacted] Policy mentions collecting "the smallest separable subset of data containing the information necessary to achieve [redacted] intelligence collection mission."[319] The "smallest separable subset . . . necessary" standard represents a thoughtful balance between a USP's interest in privacy and the imperatives of counterterrorism, even though its application is not expressly required by the [redacted] Policy.

[redacted] The "reasonable steps" requirement does not always result in collecting a smaller subset of information. In practice, operational concerns, such as the safety of a human source, can limit the scope of collection.[320] [redacted] said that the "smallest separable subset" often amounts to [redacted] explained, it may be too risky to the source to acquire only specific records.[321] Illustrating a different circumstance, [redacted] explained that CIA personnel conducting technical operations [redacted] would try to avoid [redacted] containing USP records.[322] However, [redacted] representatives have indicated that USP records are often intermingled with other records, making separation of those records infeasible at the time of collection.

[redacted] Thus, in many instances, operational concerns might lead [redacted] collecting non-pertinent information concerning USPs. The Board notes that this outcome is not contrary to the [redacted] Policy, as the policy requires only "reasonable steps" rather than a substantive outcome (*e.g.* the smallest subset necessary to the mission). [redacted] complies with the [redacted] Policy by making a reasonable attempt to limit collection; it would not be "reasonable" to limit the scope of collection where practical concerns make scoping infeasible or impossible.

[redacted] Whether the reasonable steps requirement imposes a meaningful limit on the quantity of incidental USP information [redacted] collects also depends on what constitutes "non-pertinent information that is of little or no intelligence value." Although [redacted] official described a

317 [redacted]

318 [redacted]

319 [redacted]

320 (U//FOUO) CIA and PCLOB discussion, 8/18/16.

321 [redacted]

322 [redacted]

[redacted]

[redacted]

general ethos of avoiding or limiting the collection of USP information, that same official also expressed that incidentally or accidentally collected information is potentially valuable.[323]

a) (U//FOUO) New AG Procedures

[redacted]The New Procedures change existing policy in two ways. First, the New Procedures expressly recognize that collections do include incidentally collected USP information and describe how the procedures apply to such information.[324] As mentioned above, E.O. 12333 and Annex A of the current procedures[325] require the "least intrusive technique feasible" only for collections within the United States or directed at USPs abroad.[326] The New Procedures state that "unevaluated information is presumed to include incidentally acquired information concerning U.S. persons, and to be subject to these procedures regardless of the location of the initial collection[.]"[327] The Board understands this to mean that the "least intrusive means" language will apply to all collections containing USP information, including collections conducted abroad that are anticipated to contain incidentally-collected USP data. The procedures retain the [redacted]framework for determining the least intrusive technique by category, however, and do not include a requirement that personnel further delineate techniques within each category unless feasible in the circumstances. As such, as a matter of practice, [redacted] may choose any collection technique within the applicable category when it is not feasible [redacted] to determine that a particular collection technique is more or less intrusive than another technique in the same category.

(U//FOUO) Second, the New Procedures limit collections to "only the amount of information reasonably necessary to support th[e] purpose [of the collection]."[328] For collections made without a discriminant that are too large to review immediately, or that are determined to qualify for retention without individualized review, the procedures require extra documentation. Specifically, CIA employees are required to document "[t]he collection technique(s) employed, including any reasonable steps that are or will be taken to limit the information to the smallest separable subset of data containing the information necessary to achieve the purpose of the collection."[329]

---

323 (U) *Supra* p. 24.

324 (U//FOUO) New Procedures §§ 3.2, 12.22.

325 (U//FOUO) The current procedures [redacted] consist of AR 2-2 and its annexes, including Annex A, one of the two parts of the CIA's Attorney General-approved procedures [redacted]

326 (U) Annex A § IV.D.

327 (U) New Procedures, §§ 3 ("Unevaluated information is presumed to include incidentally acquired information concerning U.S. persons, and to be subject to these Procedures regardless of the location of the initial collection[.]"), 4.1.

328 (U//FOUO) New Procedures § 3.3. The purpose of the collection must be "consistent with the CIA authorities and responsibilities described in Section 2." *Id.*

329 (U//FOUO) New Procedures § 5.

[redacted]

[redacted]

2. (U//FOUO) Recommendation 1: Require additional implementing guidance regarding reasonable steps to limit collection of USP information.

[redacted] Beyond the requirements under the New Procedures, the Board recommends [redacted] issue further guidance implementing the requirement of the New Procedures designed to limit the collection of USP data not responsive to the purpose of the collection. This could be accomplished by supplementing the [redacted] Policy or revising it once the New Procedures are finalized. In any event, the CIA has acknowledged that it will have to consider the continuing applicability of the [redacted] Policy once the New Procedures are finalized.

B. (U//FOUO) Use of USP information

[redacted] Measures to protect USP information *after* it is acquired are particularly important if [redacted] practice continues to rely on regular collection abroad that includes an unknown amount of incidentally collected USP information.

1. (U//FOUO) Analysis based on existing policy

[redacted] The rules in Annex A and the [redacted] Policy largely focus on collection, retention, and dissemination. These policies do not directly address certain key aspects of handling and use – activities that impact the privacy of USPs whose information has been collected incidentally.

[redacted] For example, although informal practice may explicitly address them, Annex A and the [redacted] Policy are silent on queries designed to return USP information. A significant amount of covered data, [redacted] is subject to queries as a means of analysis, but this routine activity is not explicitly reflected in Annex A or the [redacted] Policy. With regard to audits, the [redacted] Policy requires only maintenance of "an auditable record" of user activity for certain segregated databases "to the extent practicable."[330]

2. (U//FOUO) New AG Procedures

[redacted] Many of these issues are expected to be remedied once the CIA implements the New Procedures, as discussed below. First, the New Procedures provide access and querying requirements for unevaluated information when it is "impractical, infeasible, or detrimental to the CIA's mission to determine promptly whether the information qualified for [permanent]

330 [redacted]

[redacted]

[redacted]

retention[.]"[331] The New Procedures delineate "exceptional handling requirements" for unevaluated information that constitutes communications acquired without consent of a party or information anticipated to contain substantial USP identifying information,[332] and "routine handling requirements" for any other unevaluated information.[333]

[redacted]The Board notes that much[redacted] structured, unevaluated data likely constitutes information subject to routine handling requirements. This is because information containing a high volume of USP information may be treated under routine handling requirements if USP identifying information has been masked.[334] Routine handling requirements mandate maintaining an auditable record of activity, including access, queries designed to elicit USP information, and justification for those queries that articulates what the CIA knows or reasonably believes about the USP.[335] A CIA employee may query information subject to routine handling as long as the query is reasonably designed to retrieve information related to an authorized activity of the CIA.[336]

[redacted] The New Procedures also require that agency "information systems . . . be designed to facilitate auditing of access to and queries of information" and state that "these systems shall be audited periodically by the appropriate oversight entities."[337]

3. (U//FOUO) Recommendation 2: Formalize existing standards governing queries designed to return USP information.

[redacted] As described above, the CIA instructs [redacted] on the standard for requesting that USP information be unmasked through an online tool.[338] Additionally, the New Procedures introduce heightened requirements for queries of unevaluated information covered by the procedures' "exceptional handling requirements."[339] The Board appreciates this aspect of the New Procedures and recommends supplementing existing [redacted]protocol.

[redacted]Lower level implementing guidance should formalize [redacted]informal practices. As a general matter, incorporating existing safeguards related to use – *e.g.*, access to information, unmasking, and queries – into formal, written policy documents promotes awareness of and adherence to the rule and ensures that any future revision to the rule is subject to an appropriate balancing of equities. The Board recommends that the CIA explicitly tie queries to the CIA's

331 (U//FOUO) New Procedures § 6.
332 (U//FOUO) New Procedures § 6.2.
333 (U//FOUO) New Procedures § 6.3.
334 (U//FOUO) New Procedures § 6.3.1(b).
335 (U//FOUO) New Procedures § 6.3.3.
336 (U//FOUO) New Procedures § 6.3.4.
337 (U//FOUO) New Procedures § 10.1. The New Procedures list a variety of internal and external oversight entities that may have some role in oversight. *Id.* at § 10.2.
338 [redacted]
339 [redacted]

[redacted]

[redacted]

mission in order to clarify how authority (or limitations on that authority) flow from high level policies, such as E.O. 12333, to more granular procedures. The Board does not anticipate that adopting this recommendation would require a change [redacted] practices.

C. (U//FOUO) Retention of unevaluated USP information

[redacted] The [redacted] Policy governs a substantial amount of financial intelligence that [redacted] stores as unevaluated information. Under this policy, sets of aggregate data "that exceed the CIA's capacity to immediately review and minimize the information in its entirety upon receipt" must be stored in segregated databases until they are reviewed and minimized or deleted.[340] As discussed above, this policy [redacted] general retention framework – are structured differently from Annex A. This difference makes retention a particularly complex part of the intelligence cycle [redacted]

1. (U//FOUO) Analysis based on existing policy

[redacted] For some of its unevaluated E.O. 12333 financial intelligence, [redacted] applies fixed retention periods. Subject to certain exceptions, these retention periods are either five or twenty-five years.[341] [redacted]

[redacted][2] For other E.O. 12333 financial data sets, such as those in which the CIA masks or deletes presumed USP identifying information, the CIA interprets Annex A's enumerated retention categories to permit the indefinite retention of unevaluated USP information.[343] [redacted]

(U//FOUO) Longer retention periods raise greater privacy and civil liberties risks for any USPs whose information is incidentally collected, both by allowing for additional intelligence uses of the information and also by increasing the risk of misuse or inappropriate disclosure. Such risks may be justified if retention periods are grounded in operational needs to retain data for longer periods of time.

340 [redacted]

341 [redacted]

342 [redacted]

343 (U) *See* Annex A § VI.A.1(d)-(e); [redacted]

344 [redacted]

[redacted]

[redacted]

[redacted]The Board understands that data older than five years has been useful. But the Board also notes [redacted] does not regularly evaluate the period for which its E.O. 12333 financial intelligence tends to be valuable [redacted] now considering mechanisms to develop such evaluations. This exercise is intended to improve requests to extend retention periods, but not to better understand whether retention periods are generally set at an appropriate length.[345]

2. (U//FOUO) New AG Procedures

[redacted] As with Annex A, the New Procedures permit evaluated information to be retained indefinitely. The New Procedures define evaluated information as information that has been reviewed to determine whether it: (1) relates to an authority and responsibility of the CIA; (2) contains USP information; and (3) meets retention criteria.[346] But the New Procedures are clearer than Annex A in several regards. Notably, unlike Annex A, the New Procedures explicitly refer to the requirement that retained information must relate to an authority and responsibility of the CIA.

[redacted] More significantly, the New AG Procedures create two new retention rules for unevaluated information. Unevaluated information subject to exceptional handling requirements, such as information anticipated to contain significant USP identifying information, must be destroyed "no later than five years after the information has been made available to CIA personnel for operational or analytic use."[347] In contrast, unevaluated data subject to routine handling requirements – including unevaluated information in which the CIA has masked USP identifying information – must be deleted "no later than twenty-five years after the information is made available to CIA personnel with access to the relevant information repository."[348] All unevaluated information must be subject to either exceptional or routine handling requirements.

3. [redacted]Recommendation 3: Require periodic evaluation of the duration for which unevaluated financial data is retained.

[redacted] should evaluate and periodically reevaluate the length of time for which it retains unevaluated E.O. 12333 financial data that contains incidentally collected USP information. This evaluation should consider whether retention periods should be shorter *or* longer. The evaluation should be based on analysis regarding the sensitivity of financial information as well as how long after collection financial data remains valuable for the CIA's mission. Such evaluation will ensure that [redacted]periods for holding unevaluated USP information appropriately balance the potential need for USP information and the privacy risks associated with storing it.

---

345 [redacted].

346 (U//FOUO) New Procedures §§ 7, 12.11, 12.21.

347 (U//FOUO) New Procedures § 6.3.3.3.

348 (U//FOUO) New Procedures §§ 6.3.2, 6.3.3.2.

[redacted]

[redacted]

4. [redacted]Recommendation 4: Develop a systematic, value-based method of determining the retention period of financial data sets consistent with the New Procedures.

[redacted]The Board urges the CIA to adjust retention limitations based on the value of each data set. In order to determine how a data set should be classified under the New Procedures, CIA may be required to develop a way to systematically evaluate the quantity of sensitive information contained in new collections. Developing systematic evaluations of the value [redacted] E.O. 12333 financial intelligence may be challenging but is also consistent with other IC efforts to manage large and disparate collection activities and databases. In other contexts, government agencies have evaluated the usefulness of certain financial data collections.[redacted] These approaches may inform the CIA's consideration of mechanisms for evaluating the utility [redacted] E.O. 12333 financial intelligence.

D. (U) The relationship between existing policies and practices

[redacted]As discussed above, [redacted] governed by a number of different policies and procedures, including E.O. 12333, the current AG-approved Procedures, and lower-level procedures such as the [redacted] Policy. In most cases, there is a hierarchy to these rules. For example, AG Procedures are subordinate to E.O. 12333, which itself is constrained by any statutory rules or limitations and by the Constitution. The existence of so many policies is in many ways a

---

349 [redacted] CIA and PCLOB discussion, 9/29/15.

350 [redacted]

[redacted]

necessity; no single policy could provide detailed rules for the numerous agencies within the Intelligence Community and the diverse of activities in which they engage. As a result, virtually every discrete decision to collect, use, or retain information within the CIA is subject to numerous policies.

1. (U//FOUO) Analysis based on existing policy

The Board's review of policies and conversations with staff revealed ambiguities regarding the requirements for protecting USP information. For example, Annex A enumerates bases under which the CIA can retain USP information relies on certain Annex A bases, including one allowing information to be retained for a "reasonable period" for review and one allowing information to be retained if certain USP identifying information is deleted. However, neither of these Annex A bases maps clearly to Section 2.3 of E.O. 12333, the section that enumerates types of USP information that may collected, retained, and disseminated.

The Board understands how the Annex A bases might be reconciled with this E.O. 12333 list: Storage and maintenance for the purpose of evaluating data may be implied from Section 2.3's substantive categories (*e.g.* foreign intelligence), and retention of information concerning a USP in which the USP identifying information has been deleted arguably does not implicate that USP's privacy.

The relationship between practices and some of the current policies regarding the handling of USP information is also not clear. Three examples illustrate this concern. First, Annex A permits indefinite retention in certain instances in which processing the data sufficiently protects the USP, such as when USP identifying information is masked or deleted; in contrast, is ambiguous with regard to whether masking permits the CIA to retain suggests that masking and deletion are equivalent. This potential discrepancy is important because represents that which includes at least some information satisfies retention requirements by masking USP identifying information decision to mask data is rooted in a practical concern: can retrieve and use USP identifying information that is *masked*, while USP identifying information that is permanently *deleted* would be unusable. The Board notes that user might seek to retrieve USP identifying information – to unmask the financial intelligence – if there is a need to know, *i.e.* when the USP identifying information itself constitutes foreign intelligence.

Second, the Policy's protections are based on minimization and segregation. Its definition of "minimization" would require permanently delete identifying USP information from unevaluated data. Although relies heavily on the policy in carrying out the covered activities, has not adopted the Policy's

[redacted]

definition of "minimize" because, as described above, the CIA recognizes that the policy's definition of "minimization" does not capture the full range of safeguards that may be applied to collected information.

[redacted]Third,[redacted] has recently introduced user agreements for personnel accessing unevaluated unstructured data sets. While the user agreements make repeated reference to the requirements of AR 2-2, these agreements do not reflect a key protection [redacted]has described: the requirement for users to identify any potential USP information that they happen upon so the information can be masked.

[redacted] training practices do not remedy the aforementioned ambiguities and uncertainties. As described above, [redacted]has not identified a comprehensive, mandatory training that covers handling of USP information, the incidental collection of USP information, and the querying of such data. Although other trainings cover the topic more extensively, these trainings are optional. It follows that not all [redacted]employees are provided trainings that fully synthesize existing, written policies and procedures or describe informal rules relating to those policies and procedures.[351]

[redacted]Ambiguities regarding the handling of USP information can pose a risk to USPs' privacy and civil liberties. CIA employees may find it difficult to determine what they are permitted to do and when to implement safeguards. [redacted]managers have said that their personnel know to contact an attorney with any questions, particularly when USP information is involved.[352] But the Board believes that an informal understanding is often a poor substitute for written policies. Absent such policies, well-meaning CIA employees may either accidentally bypass important requirements or unduly restrict their own use of important information. Furthermore, the ambiguities regarding how different policies relate to each other can leave managers and attorneys uncertain about the continuing importance of specific policies aimed at protecting USP information.

2. (U//FOUO) New AG Procedures

(U//FOUO) In many ways, the New Procedures are much clearer than AR 2-2 and its Annexes. Several definitions have been added or expanded upon,[353] and protocols for bulk collection and the storage of unevaluated information are substantially more detailed.[354] Moreover, the New Procedures acknowledge the existence of other authorities.[355]

---

351 [redacted]

352 [redacted]

353 (U//FOUO) New Procedures § 12 (defining for the first time, for example, bulk collection (§ 12.2), dissemination (§ 12.8), unevaluated information (§ 12.22), U.S. Person identifying information (§ 12.25)).

354 (U//FOUO) New Procedures §§ 5, 6.

355 [redacted] *See, e.g.*, New Procedures § 4 (authorizing collection with a nexus to a CIA mission requirement and a CIA responsibility under the National Security Act of 1947 and Executive Order 12333).

[redacted]

[redacted]

3. [redacted] Recommendation 5: Review, reconcile, and clarify policies governing [redacted] relationship to each other.

[redacted]In cooperation with other CIA components as necessary,[redacted] should undertake a comprehensive review of lower level policies and practices regarding the handling of USP information to ensure that: (1) key terms are defined in writing; (2) relationships among policies are clearly defined; and (3) interpretations in writing match actual practice. The Board recognizes that implementing the New Procedures will eliminate some of the aforementioned ambiguities.

Fully addressing the Board's concern, however, requires, further review of relevant implementing policies, practices, and training. Policies that complement, implement, or refer to relevant portions of E.O. 12333 or the New Procedures should make clear their relationship to these two key authorities and use language consistent with them. Supplemental policies should also provide any[redacted] definitions and instructions needed to clarify how the New Procedures apply [redacted] Additionally, training and reference documents should reflect not only the New Procedures but also related interpretations and subordinate policies and the relationships among them.

4. [redacted]Recommendation 6: Require additional training for [redacted] employees about governing policies and how different policies relate to each other.

[redacted] staff should receive regular training and usable reference materials or other reminders that reflect all key rules and practices applicable to the collection, retention, exploitation, and dissemination of USP information that is collected incidentally. In general, these trainings should reflect [redacted] legal staff's synthesis of the disparate written policies and procedures that govern handing of USP information. It is important that staff understand the full range of rules applicable to them, even if these rules come from multiple sources.

[redacted]

[redacted]

Annex: (U) Separate Statement of Board Members Wald and Dempsey

[redacted] We appreciate the detailed analysis contained in the Board's report and strongly support its recommendations. If implemented, these recommendations will promote further accountability [redacted] and establish additional protections for USP information.

[redacted]

[redacted] we believe [redacted] should take several additional steps to ensure that USP information is adequately protected. These additional recommendations are based on staff research and documents as well as Board participation in briefings with the CIA.

[redacted]**Documentation.** Given the CIA's regular practice of acquiring datasets [redacted] of incidentally-collected USP information, the CIA should require additional documentation throughout the intelligence process. Such documentation will not only promote adherence to safeguards already in place but also will create an audit trail so the agency can continue to provide sufficient internal oversight of its own activities. We believe requiring documentation would be particularly beneficial in three contexts.

[redacted] First, consistent with their current practice and policy,[redacted] should continue to document the justification for acquiring any dataset, e.g. the foreign intelligence purpose, when initiating a collection. As currently required, and as will be required under the New Procedures, this justification should clarify the anticipated value of the dataset[redacted]

[redacted] Second, when processing the data and ultimately retaining it, [redacted]should document: (1) that an analyst considered whether the purpose of the collection could be achieved by acquiring a smaller subset, and the outcome of that determination; and (2) a determination that the collected intelligence is likely to have ongoing value and therefore is suitable for retention for the purpose of evaluation.

[redacted] Third, users[redacted] should document the mission-related justification for queries designed to return USP data. We would require this documentation regardless of whether the user is inside the CIA. The requirement should involve

[redacted]

[redacted]

documentation with a high level of granularity. For instance, if the mission-related justification is the expectation of obtaining foreign intelligence, the user should indicate why the USP identifying information used to query a database is likely to return foreign intelligence information. [redacted]

[redacted]**Training.** We understand tha [redacted] legal staff are the first line of defense for legal and policy compliance, and appreciate the efforts of these individuals to safeguard privacy and civil liberties while also promoting the CIA's mission. The existing AG-approved procedures and implementing procedures are complicated, confusing, and in some places, ambiguous. Although the New Procedures clarify the rules substantially, [redacted] could better support its legal staff in their important role by implementing trainings that directly address the nuances of these policies and how they fit together. These trainings should be conducted regularly and include usable reference materials or other reminders that reflect all key rules and practices applicable to the collection, retention, exploitation, and dissemination of USP information that is collected incidentally.

[redacted] By implementing these additional recommendations, [redacted] can help ensure that USP information is protected in the coming years. We do not believe these recommendations will be unduly burdensome to implement. In fact, the approval of the new, much-improved procedures presents the CIA with a nearly unprecedented opportunity to remedy existing issues and establish controls within the agency's legal framework to prevent new issues from arising in the future. We hope that the CIA seizes this opportunity by implementing the recommendations in the Board's report, the additional recommendations outlined above, and similar reforms throughout the agency.

356 [redacted]

[redacted]