Privacy and Civil Liberties Oversight Board

Executive Order 12333

Board Members

Adam I. Klein, Chairman

Jane E. Nitze

Edward W. Felten

Travis LeBlanc

Aditya Bamzai

The Board acknowledges with gratitude the staff members who worked on this project, including Matthew Eldred and Justin Hemmings, Board Counselors, and other current and former staff members.

Table of Contents

Introduction **4**

I. The Board's Examination of Counterterrorism-Related Activities Conducted Under EO 12333 ..... **5**

A. Background 5

B. Public Engagement 6

C. Deep Dive Reviews 7

1. CIA Deep Dive I 7

2. CIA Deep Dive II 7

3. Deep Dive into NSA's Use of XKEYSCORE as an Analytic Tool 8

D. Attorney General-Approved Guidelines under EO 12333 9

E. General Observations 11

II. Executive Order 12333 ..... **13**

A. History 13

B. The Contents of EO 12333 14

1. Goals, Directions, and Responsibilities 15

2. Conduct of Intelligence Activities 17

3. General Provisions 19

C. The Broader Legal Context 19

III. Frequently Asked Questions **20**

Introduction

The Privacy and Civil Liberties Oversight Board ("Board") presents this report as a capstone to its more than six-year examination of the government's use of Executive Order 12333 ("Order" or "EO 12333").[1] The Order is a foundational document for the United States' foreign intelligence efforts, including efforts to protect the nation from terrorism.[2] It establishes a framework that applies broadly to the government's collection, analysis, and use of foreign intelligence and counterintelligence—from human sources, by interception of communications, by cameras and other sensors on satellites and aerial systems, and through relationships with intelligence services of other governments.

As such, the Order is among the largest and most complex of U.S. surveillance authorities. Unlike certain provisions of the Foreign Intelligence Surveillance Act ("FISA") that were the subject of the previous Board reports, the Order does not authorize one specific foreign intelligence program. Rather, it provides a broad framework for the organization and coordination of missions of the Intelligence Community ("IC"). In addition, the Order authorizes various forms of collection, constructs administrative and oversight infrastructure, and outlines protections for U.S. persons.[3]

This report seeks to inform policymakers and the public about the Order in two ways.[4] First, it describes the Board's examination of the government's use of the Order. Second, the report provides an overview of the Order.

Section I provides an overview of the Board's examination of certain counterterrorism activities conducted under the Order. This examination included public events to receive public and non-government organization views, Board staff research, and three classified "deep dive" reviews into activities conducted under the Order by the Central Intelligence Agency ("CIA") and the National Security Agency ("NSA"). The Board also advised agencies about how to protect privacy and civil liberties as they drafted or updated Attorney General-

---

[1] The Board is an independent agency within the executive branch, established pursuant to the Implementing Recommendations of the 9/11 Commission Act of 2007. *See* Pub. L. No. 110-53 § 801, 121 Stat. 266, 352 (2007). The bipartisan, five-member Board is appointed by the President and confirmed by the Senate.

[2] Exec. Order 12,333, 46 Fed. Reg. 235 (Dec. 8, 1981), https://www.dni.gov/index.php/ic-legal-reference-book/executive-order-12333.

[3] EO 12333 defines a U.S. person as "a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments." Exec. Order 12333 § 3.4(i).

[4] *See* 42 U.S.C. § 2000ee(f) ("The Board (1) shall make its reports, including its reports to Congress, available to the public to the greatest extent that is consistent with the protection of classified information and applicable law; and (2) shall hold public hearings and otherwise inform the public of its activities, as appropriate and in a manner consistent with the protection of classified information and applicable law, but may, notwithstanding section 552b of title 5, meet or otherwise communicate in any number to confer or deliberate in a manner that is closed to the public.").

approved guidelines required under the Order. In the past four years, the Board advised seven agencies or components on new or revised guidelines. These summaries are presented at a high level to protect privileged and classified information.

Section II summarizes the history, structure, and content of the Order, focusing on the Order's safeguards for privacy and civil liberties. Section III answers frequently asked questions about the Order.

When the previous Board embarked on this project in 2015, it anticipated that most of what the Board would learn through its oversight projects would be classified or otherwise protected information. This has proven true. Accordingly, a detailed accounting of our work is not possible. Nevertheless, in this capstone report, we have summarized the Order and, where possible, provided unclassified examples and descriptions of the Board's work to date.

The Board's in-depth review of three activities conducted pursuant to the Order, in addition to its advice engagements on Attorney General-approved guidelines, shed meaningful light on how the IC implements the Order. Because EO 12333 governs so much of the United States' intelligence activities, and is implemented by seventeen different elements of the IC, the Board's review necessarily did not cover the full extent of the framework provided for, and activities conducted under, the Order. The Board anticipates that it will continue to encounter EO 12333 in its work.

I. The Board's Examination of Counterterrorism-Related Activities Conducted Under EO 12333

A. Background

On July 23, 2014, the Board announced that it would examine the Order and its implications for privacy and civil liberties.[5] Later that same year, on December 17, the Board convened a meeting to hear the views of non-government organizations and academics.[6] The Board next received classified briefings from intelligence agencies on individual intelligence missions and certain specific counterterrorism-related activities conducted pursuant to the Order. Throughout, the Board reviewed relevant documents, including agencies' EO 12333 implementing procedures.

[5] Privacy and Civil Liberties Oversight Board Public Meeting, Washington, DC (July 23, 2014), https://web.archive.org/web/20200610093555/www.pclob.gov/events/2014/july23.html.

[6] Meeting Summary, Board meeting with NGOs on EO 12333 (Dec. 17, 2014), https://web.archive.org/web/20200610094757/https://www.pclob.gov/library/20141217-EO12333-NGOMeeting.pdf.

The following April, the Board adopted a project description for examining specific counterterrorism-related activities under the Order.[7] The Board anticipated that its examination would result in a public report concerning how the Order governs the collection, use, dissemination, and retention of intelligence information.[8] Since then, the Board has completed three classified deep dive reviews and advised agencies on the revisions to, or in some instances drafting of, their Attorney General-approved guidelines implementing the Order. Recognizing that the deep dive reviews could cover only a fraction of the activities conducted under the Order, the Board selected the oversight topics with care. The Board chose to review counterterrorism-related activities involving one or more of the following: (1) bulk collection that carries a significant chance of acquiring some U.S. person information; (2) use of incidentally collected U.S. person information; (3) targeting of U.S. persons; and (4) collection that occurs within the United States or from U.S. companies.

Based on these criteria, the Board conducted two deep dive reviews of CIA activities, and one review of an NSA activity. The Board assessed the counterterrorism value of the activities in question, their impact on privacy and civil liberties, and whether those national security activities were appropriately balanced with privacy and civil liberties. The Board also considered whether the activities comport with requirements imposed by the Constitution, statutes, and agency-level implementing procedures and guidelines. The Board completed its deep dive review of one CIA activity in 2017 and its deep dive review of the NSA activity in 2020. Both reviews resulted in classified reports. The Board provided both classified reports to Congress, and the NSA and CIA reports to the respective agencies. Also in 2020, staff completed the deep dive review of the second CIA activity.

B. Public Engagement

The Board sought the perspectives of experts regarding the scope of its inquiry, what issues to consider, and stakeholders' interests. In addition to the Board's 2014 public meeting, the Board hosted a public event on May 13, 2015, at the National Constitution Center in Philadelphia. The event featured panel discussions with academics, non-government organization representatives, and former government officials on the constitutional implications of EO 12333 and the practical uses of the authority.[9] In addition to this meeting,

---

[7] The Board did so by a 4-1 vote. Board Member Rachel Brand voted against the project description for reasons outlined in a separate statement. *See* Rachel Brand, Board Member, Privacy and Civil Liberties Oversight Board, Statement at Public Meeting (Apr. 8, 2015), https://documents.pclob.gov/prod/Documents/EventsAndPress/7a37a2b4-6702-45c6-ae9b-b811dd1dcd71/20150408-Statement-Brand.pdf.

[8] *See* PCLOB Examination of E.O. 12333 Activities in 2014 https://documents.pclob.gov/prod/Documents/EventsAndPress/b7b559bb-6687-4638-a7af-f40f2f9ae09a/20150408-EO12333_Project_Description.pdf.

[9] The Board is grateful to all those who contributed to this event.

the Board also solicited and received 41 public comments on its review of the Order and met with representatives of nongovernmental organizations and other stakeholders.[10]

These outside perspectives represented a broad array of institutional and individual stakeholders inside and outside the United States, and the Board appreciates the time and work contributed by all the participants.

C. Deep Dive Reviews

As noted previously, pursuant to its statutory mandate, the Board conducted three classified deep dive reviews into intelligence activities conducted for counterterrorism purposes under the Order. The Board examined two activities conducted by the CIA and one by the NSA. The topics of the two CIA deep dive investigations remain classified; the third deep dive concerns NSA's use of XKEYSCORE as an intelligence analysis tool. Each deep dive investigation involved rigorous fact gathering and, where appropriate, provided recommendations to the agency.

1. CIA Deep Dive I

For CIA Deep Dive I, which concerned a classified program, the Board received briefings from and held meetings with CIA staff between April 2015 and August 2016. The Board also received and reviewed relevant documents from the CIA, the CIA Office of the Inspector General, and other relevant executive branch agencies.

The Board completed a report on this activity in 2017. That report was provided to the DNI, CIA, and Congress. It included a detailed explanation of the activity and recommendations to improve the protection of privacy and civil liberties. The Board's review concentrated on the protection of U.S. persons' privacy and civil liberties. Since completion of the review CIA has implemented, or implemented in part, all the Board's recommendations.

2. CIA Deep Dive II

Between August 2015 and December 2016, the Board gathered information relevant to CIA Deep Dive II, concerning another classified program, in coordination with the CIA's Office of Privacy and Civil Liberties. This included a series of classified briefings, demonstrations, follow-up sessions, and meetings with CIA personnel. The Board also received and reviewed documents and written responses to the Board's information requests. Documents reviewed included relevant training documents, database user manuals, lower-level implementing procedures, and statistics. Again, the Board concentrated on the protection of U.S. persons' privacy and civil liberties.

[10] Notice of Activities under Executive Order 12333, 80 Fed. Reg. 15259 (Mar. 23, 2015), https://www.govinfo.gov/content/pkg/FR-2015-03-23/pdf/2015-06537.pdf.

While the Board was conducting this review, the CIA revised its Attorney General-approved EO 12333 procedures, which were issued and last updated in the 1980s.[11] As with all IC elements, these procedures are the primary source of protections afforded to U.S. persons with respect to activities conducted by the CIA under the Order. CIA Deep Dive I was completed before the new guidelines were issued. Execution and implementation of the revised guidelines impacted CIA Deep Dive II.

The investigation and review continued through 2017; however, the Board lost its quorum that year and did not regain a quorum until late the following year. During the interim period, Board staff continued to review the information gathered, including application of the revised Attorney General-approved guidelines to the deep dive activity, and began to write a report. In 2020, staff again engaged with the CIA to address a few outstanding factual questions and determined that the staff draft of the report remained factually accurate as of when it was previously reviewed by CIA. Accordingly, a staff report explaining the activities and providing recommendations was transmitted in late 2020. The classified report was delivered to the CIA and Congress.

3. Deep Dive into NSA's Use of XKEYSCORE as an Analytic Tool

The NSA deep dive concerned NSA's use of XKEYSCORE, an intelligence analysis tool. The Board received briefings from and held meetings with NSA staff between May 2015 and November 2016. The Board also reviewed the guidance and training provided to NSA personnel, compliance mechanisms, and the relationship between the NSA activity and the NSA's EO 12333 implementing procedures.

In early 2019, after the Board regained a quorum, the Board reengaged with the NSA and received additional briefings, demonstrations, and information. During this process, the Board worked with NSA to confirm and update facts provided in the 2015 timeframe. Again, the Board concentrated on the protection of U.S. persons' privacy and civil liberties.

The Board produced a detailed, classified report explaining NSA's use of XKEYSCORE as an analytic tool and relevant privacy and civil liberties protections in late 2020. Accompanying the report were recommendations from the Board and additional views of individual Board Members. The report and recommendations were delivered to the NSA, Congress, and other relevant executive branch agencies.

[11] CIA, Central Intelligence Agency Intelligence Activities: Procedures Approved by the Attorney General Pursuant to Executive Order 12333 (CIA AG Guidelines) (Jan. 18, 2017), https://www.cia.gov/about-cia/privacy-and-civil-liberties/CIA-AG-Guidelines-Signed.pdf.

D. Attorney General-Approved Guidelines under EO 12333

The Order authorizes the collection and use of information concerning U.S. persons only in accordance with Attorney General-approved guidelines.[12] The Order specifies the types of information concerning U.S. persons that such procedures must permit to be collected, retained, and disseminated.[13] And the Order prohibits the use of specified collection techniques except in accordance with Attorney General-approved guidelines.

The Order further limits the types of collection techniques the guidelines may authorize for certain IC elements and where they may be conducted. For example, the guidelines may not authorize "[t]he Central Intelligence Agency (CIA) to engage in electronic surveillance within the United States except for the purpose of training, testing, or conducting countermeasures to hostile electronic surveillance." Finally, the Order requires Attorney General-approved guidelines for the sharing of raw signals intelligence.

Attorney General-approved guidelines play an important role in establishing each element's safeguards for the privacy and civil liberties of U.S. persons. The Guidelines also comply with constitutional and other legal requirements.[14]

After President Reagan issued EO 12333 in 1981, members of the IC prepared implementing guidelines and obtained Attorney General approval for them.

---

[12] Exec. Order 12333 §§ 2.3, 2.4. Specifically, Section 2.3 of EO 12333 authorizes intelligence agencies to "collect, retain, or disseminate information concerning United States persons" only in accordance with procedures established by the head of the agency and approved by the Attorney General, after consultation with the Director of National Intelligence. Any such procedures "shall" permit collection, retention, and dissemination of certain types of information concerning U.S. persons, including information "constituting foreign intelligence" and information "obtained in the course of a lawful foreign intelligence, counterintelligence, international drug or international terrorism investigation." Section 2.4 authorizes intelligence agencies "to use such techniques as electronic surveillance, unconsented physical searches, mail surveillance, physical surveillance, or monitoring devices," within the United States or directed against a U.S. person abroad, only in accordance with the Attorney General-approved guidelines.

[13] *Id.* at § 2.3. While the Order lists ten types of information that must be permitted to be collected, retained, and disseminated, agencies do collect, disseminate, and retain other types under other legal authorities.

[14] *See id.* at § 2.8. Nothing in EO 12333 "shall be construed to authorize any activity in violation of the Constitution or statutes of the United States." *Id.* The Attorney General-approved guidelines "shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes." *Id.* § 2.4.

When the Board began its review, some agencies, including the CIA and the NSA,[15] had not updated their Attorney General-approved guidelines since the 1980s.[16] And still others had not developed Attorney General-approved guidelines at all. When the Board began this examination, the IC elements within the Department of Treasury, the Drug Enforcement Administration, and the Department of Homeland Security ("DHS") (including its Office of Intelligence Analysis and the intelligence elements of the Coast Guard) were all operating pursuant to interim guidelines or other procedures.[17]

In part because they were outdated, many agencies' Attorney General-approved guidelines did not reflect contemporary technology or intelligence-gathering methods. Instead, they reflected a global communications and technology landscape vastly different from today, and an outmoded governmental capacity to collect, process, store, and analyze information. When most agencies' Attorney General-approved guidelines were written, telephone conversations typically occurred on landline phones, and written messages were sent by fax, telegram, or Telex. Today's worldwide network of fiber-optic cables transmitting both oral and written communications had not yet come into existence; nor had the commercial Internet, and with it the widespread use of email, instant messages, video chats, and social media. The Internet had not taken hold as the primary means through which individuals seek out information, nor as a prominent method of communicating and engaging in commerce. Most people stored their photographs, documents, and communications in their homes, not in "the cloud." Mobile phones were uncommon, and smart devices had not yet been invented. It is important for intelligence agencies to leverage technological advances to meet their mission needs. When intelligence agencies apply guidelines that do not consider the evolution of technology, the privacy and civil liberties safeguards in those guidelines may no longer be appropriately balanced with the practical realities of information-gathering practices in the digital age. Accordingly, in March 2013, at the Board's request, the Department of Justice briefed the Board on the status of ongoing efforts to modernize the

[15] When the Board began its review in 2014, the procedures governing the Department of Defense had been approved in 1982. The annex to those procedures, which addresses in detail the NSA's signals intelligence activities, was approved in 1988. The CIA procedures governing activities outside the United States dated to 1982, and while those governing activities inside the United States were updated more recently, most of the changes were not substantive and were made to reflect the passage of the Intelligence Reform and Terrorism Prevention Act of 2004. The procedures of the Departments of State and Energy were approved in 1989 and 1992 respectively.

[16] For a table compiled in 2017 with the names and dates of all EO 12333 implementing procedures, including links to those that are publicly available, see Status of Attorney General-Approved U.S. Person Procedures under Executive Order 12333 (May 16, 2017), https://www.dni.gov/files/CLPT/documents/Chart-of-EO-12333-AG-approved-Guidelines_May-2017.pdf.

[17] These entities were designated as IC elements in 2003.

guidelines. The Board subsequently sent a letter asking the Attorney General and the Director of National Intelligence ("DNI") to prioritize these efforts.[18]

Pursuant to 42 U.S.C. § 2000ee(d)(1), the Board can "review proposed legislation, regulations, and policies related to efforts to protect the Nation from terrorism." Under this authority, the Board has provided advice on every significant issuance or revision of Attorney General-approved guidelines under the Order. Since 2016, the Board provided advice on new or revised procedures to the Department of Defense (2016), Central Intelligence Agency (2016), Department of Energy (2016), Department of Homeland Security (2016), Department of Treasury (2019), the Coast Guard (2019), and the Office of the Director of National Intelligence (2019).[19] The Board commends these agencies for their efforts to develop new and revised guidelines.

Additionally, the Board reviewed and provided advice on procedures created in accordance with Section 2.3 of the Order to govern the dissemination of unevaluated information derived from signals intelligence ("SIGINT") activities.[20] When writing its advice and recommendations, the Board considered whether those Section 2.3 procedures appropriately considered privacy and civil liberties; it took into account the nature of the data at issue, the uses of data that the procedures authorize, the limits and inter-agency coordination that the procedures impose, and the related control mechanisms that the procedures require. Ultimately, the DNI publicly released those procedures, known as the 12333 Raw SIGINT Availability Procedures, and an accompanying fact sheet on January 12, 2017.[21]

E. General Observations

As noted previously, most of the Board's work has been classified or otherwise protected. Nonetheless, the Board offers some general observations derived from its deep dive reviews and advice engagements.

---

[18] Letter from PCLOB Chairman David Medine to Attorney General Eric Holder and Director of National Intelligence James Clapper (Aug. 22, 2013), https://www.dni.gov/files/documents/PCLOB_Letter.pdf.

[19] Board Member Elisebeth B. Collins provided advice regarding the SIGINT Annex to the Department of Defense Manual 5240.01 during the Board's sub-quorum period.

[20] *See* Exec. Order 12333 § 2.3. Section 2.3 of the Order requires that information derived from signals intelligence only be disseminated or made available in accordance with procedures established by the Director of National Intelligence in coordination with the Secretary of Defense and approved by the Attorney General. These procedures were meant to facilitate the sharing of raw signals intelligence with IC elements that had previously not had access to that type of information.

[21] Office of the Director of National Intelligence, Procedures for the Availability or Dissemination of Raw Signals Intelligence Information by the National Security Agency under Section 2.3 of Executive Order 12333 (Jan. 3, 2017), https://www.dni.gov/files/documents/icotr/RawSIGINTGuidelines-as-approved-redacted.pdf; Fact Sheet on E.O. 12333 Raw SIGINT Availability Procedures (Jan. 3, 2017), https://www.dni.gov/files/documents/icotr/FactSheetEO12333RawSIGINTProcedures.pdf.

Most agencies' Attorney General-approved guidelines provide a high-level framework for the collection, retention, and dissemination of U.S. person information. The principles in the Attorney General-approved guidelines apply broadly to the IC elements' intelligence activities. Many IC elements are divided into smaller mission components or divisions that execute specific intelligence activities. Accordingly, many IC elements rely on agency-specific implementing procedures or activity-specific policies to guide specific foreign intelligence activities conducted under the Order. Though not subject to Attorney General approval, such policies must comply with the Order and the agency's Attorney General-approved guidelines.

As agencies implement their new or revised Attorney General-approved guidelines, such lower-level policies likewise must be updated to reflect new privacy and civil liberties safeguards. For instance, some agencies' new or revised Attorney General-approved guidelines for the first time address "bulk collection." As a result, activity-specific policies that relate to such activities must be updated to address the safeguards now afforded by the revised procedures, as well as PPD-28 and other intervening developments in the law. These also may include, for example, new or revised training requirements and updated database user manuals. These updates to policies, training, manuals, and other guidance are an important mechanism for ensuring that U.S. person protections are applied appropriately at the operational level and that the policies and procedures governing those activities accurately reflect and implement the element's current Attorney General-approved guidelines and other applicable law.

Further, as IC elements work to bring their protections for U.S. persons' data into the digital age, they should do the same for the legal and constitutional analyses underlying those activities. Agencies should review their analyses regularly and revise them as necessary. Activity-specific analysis should update as appropriate to reflect changes in the law and technology. For instance, as technology evolves, so may the IC element's ability to assess the scope and nature of U.S. person information likely to be acquired incidentally while conducting a given activity. Similarly, an IC element's analytic capabilities (e.g., its ability to query or search for U.S. person information) may broaden, and short- or long-term retention capabilities may evolve. Such potential new facts could impact an existing legal analysis. Additionally, as capabilities and intelligence needs evolve, elements benefit from regularly assessing the value of a specific intelligence activity in achieving its stated purpose.

Finally, in recent years, many IC elements have updated or issued new Attorney General-approved guidelines. Some of these updates were the first since the guidelines' issuance in the 1980s. In the future, more frequent updates will likely be needed. As technology and the law evolve at an ever-faster pace, the IC's review and revision of elements' Attorney General-approved guidelines should proceed at a similar rate. Up-to-date guidelines will better safeguard U.S. persons' privacy and civil liberties and support intelligence mission needs.

II. Executive Order 12333

At a high level, the Order articulates broad principles for foreign intelligence activities, including intelligence collection that occurs outside of the territorial United States. It does not authorize any one intelligence-gathering effort, and there is no single EO 12333 surveillance "program." The Order therefore differs from statutes, such as FISA, that often provide detailed rules and procedures for individual surveillance techniques or programs.

This Section provides a brief overview of the history and content of the Order and the legal context in which it operates. Section II.A briefly explains the origins and purposes of the Order and its two predecessors, Executive Orders 12036 and 11905. Section II.B provides an overview of the Order's three parts, and Section II.C describes how the Order interacts with other legal authorities, such as FISA.

A. History

Executive orders are directives issued by the President of the United States. Executive orders "are generally directed to, and govern actions by, Government officials and agencies," not private individuals.[22] The President's power to issue executive orders derives from statutes and Article II of the Constitution.

Issued by President Reagan in 1981, the Order was the third in a line of executive orders aimed at organizing and overseeing U.S. intelligence activities. President Ford signed the first order, Executive Order 11905, in 1976 in the wake of revelations of domestic U.S. intelligence abuses.[23] President Ford's order reorganized certain parts of the IC.[24] In response to revelations about U.S. intelligence agencies' involvement in assassination plots overseas, the order also prohibited U.S. government employees from "engag[ing] in, or conspir[ing] to engage in, political assassination."[25]

Two years later, in 1978, President Carter signed Executive Order 12036 to expand Ford's order. The Carter order imposed new organization and oversight. It also included stringent requirements on when intelligence operations could target U.S. citizens.[26] Later that year, Congress passed and the President signed the Foreign Intelligence Surveillance Act of

---

[22] House Committee on Government Operations, "Executive Orders and Proclamations: A Study of a Use of Presidential Powers." U.S. GOV'T PRINTING OFFICE (1957).

[23] Christopher H. Pyle, *CONUS Intelligence: The Army Watches Civilian Politics,* WASHINGTON MONTHLY, at 4 (Jan. 1970); Seymour M. Hersh, *Huge C.I.A. Operation Reported in U.S. Against Antiwar Forces, Other Dissidents in Nixon years*, N.Y. TIMES, at A1 (Dec. 22, 1974).

[24] Exec. Order 11905 § 5(g), 41 Fed. Reg. 7703 (Feb. 18, 1976), https://www.fordlibrarymuseum.gov/library/speeches/760110e.asp.

[25] *Id.*

[26] Exec. Order 12036, 43 Fed. Reg. 3674 (Jan. 24, 1978).

1978, which imposed additional, *statutory* restrictions on certain domestic intelligence activities. Finally, in 1981, President Reagan replaced the earlier orders with EO 12333.

In 2008, President George W. Bush undertook the next major revision of the Order. The 2008 revision was needed to reflect landmark changes to the structure of the IC made by the Intelligence Reform and Terrorism Prevention Act of 2004.[27] Most notably, the Act had created a DNI and National Counterterrorism Center. These changes were based on recommendations by the 9/11 Commission, which found that stove-piping and lack of unity in the IC impeded the U.S. response to terrorism before 9/11.[28] The 2008 revision updated the Order to reflect these new institutions and to advance the goal of integrating the IC under the new DNI.[29] The 2008 revision also addressed certain privacy and civil liberties protections.[30] This amended version of the Order remains in effect today.

B. The Contents of EO 12333

EO 12333 contains three parts. Part 1 establishes the goals of U.S. intelligence and assigns roles and responsibilities to the entities that comprise the IC. That Part is discussed in Section B.1 below. Section B.2 covers EO 12333 Parts 2 and 3. Part 2 of the Order explains the need for foreign intelligence information and establishes principles that balance that need with the protection of the rights of U.S. persons. It specifically requires IC elements to adopt certain procedures for the collection, retention, and dissemination of information concerning U.S. persons and the use of specific collection techniques. EO 12333 Part 3 addresses oversight, instructs intelligence agencies on how to implement the Order, and defines certain terms.

As with other elements of U.S. law, the Order does not operate in a vacuum. Other executive orders, policy directives, statutes, or the like may impose requirements above and beyond those contained in EO 12333. For example, activities subject to FISA must also comply with that Act's requirements.[31]

---

[27] *See* Pub. L. No. 108-458, 118 Stat. 3638 (2004).

[28] *See, e.g.*, National Commission on Terrorist Attacks, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, at 403-14, 416-17 (Jul. 17, 2004).

[29] Exec. Order 13470, 3 C.F.R. 13470 (Jul. 30, 2008), https://www.govinfo.gov/content/pkg/CFR-2009-title3-vol1/pdf/CFR-2009-title3-vol1-eo13470.pdf.

[30] For example, the 2008 revision requires IC elements to consult the DNI when crafting Attorney General-approved guidelines, adds a requirement that the IC produce those guidelines to relevant congressional committees, and incorporates limitations on covert action for the purpose of influencing U.S. domestic activities. Exec. Order 13470 § 1.3(a)(2).

[31] *See generally* 50 U.S.C. § 1801 *et seq.* In addition, Presidential Policy Directive-28, or PPD-28, provides protections to non-U.S. persons in the conduct of signals intelligence activities. Each administration can adopt a different naming convention for their issued presidential directives. Regardless of name, however, presidential directives are a form of Executive Order that states the president's national security policy and requirements for the Executive Branch.

1. Goals, Directions, and Responsibilities

Part 1 of the Order describes the roles and functions of the elements of the IC. The term "Intelligence Community," or IC, refers to a specific group of entities designated in statute and executive order. Currently, there are seventeen such entities,[32] ranging from large agencies like the CIA to smaller offices within agencies like the Office of Intelligence and Analysis within DHS.[33] These entities operate as part of a unified intelligence effort to supply information to the President and senior policymakers "on which to base decisions concerning the development and conduct of foreign, defense, and economic policies, and the protection of United States national interests from foreign security threats."[34] The DNI is the head of the IC and the principal adviser to the President for intelligence matters related to national security.[35]

The Order sets forth the types of activities that IC elements are responsible to undertake. Each element is charged with collecting, analyzing, producing, and disseminating foreign intelligence and counterintelligence.[36] The Order also addresses how each element may acquire intelligence, distinguishing between intelligence that is collected "overtly," "through publicly available sources," or "through clandestine means."[37] EO 12333 does not define these three terms; however, some agencies define these terms in their individual Attorney General-approved guidelines.[38] Agencies are encouraged to pursue foreign

---

[32] The seventeen elements are the CIA; Defense Intelligence Agency; NSA; National Reconnaissance Office; National Geospatial-Intelligence Agency; intelligence and counterintelligence elements of the Army, Navy, Air Force, and Marine Corps; intelligence elements of the Federal Bureau of Investigation; intelligence and counterintelligence elements of the Coast Guard; Bureau of Intelligence and Research, Department of State; the Office of Intelligence and Analysis, Department of the Treasury; Office of National Security Intelligence, Drug Enforcement Administration; Office of Intelligence and Analysis, Department of Homeland Security; Office of Intelligence and Counterintelligence, Department of Energy; and Office of the Director of National Intelligence.

[33] The IC elements that are offices within larger agencies or departments typically act as a liaison between their department or agency and the broader IC.

[34] Exec. Order 12333 § 1.1. To accomplish these goals, Part 1 also highlights three areas of special emphasis for U.S. intelligence: (1) espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests; (2) threats to the United States and its interests from terrorism; and (3) threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction.

[35] *See id.* at § 1.3.

[36] *See id.* at § 1.7. Of note, the National Reconnaissance Office, an agency within the Department of Defense, is "responsible for research and development, acquisition, launch, deployment, and operation of overhead systems and related data processing facilities to collect intelligence and information to support national and departmental missions and other United States Government needs[.]" Exec. Order 12333 § 1.7(d).

[37] *See id.* at § 1.7. EO 12333 does not define these three terms, and definitions of the terms may vary slightly between different IC elements and contexts.

[38] For example, the CIA defines publicly available to include "information that has been published or broadcast for public consumption, is available on request to the public, is accessible online or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer (but not amounting to physical surveillance),

intelligence and counterintelligence within the defined boundaries. "All means, consistent with applicable Federal law and this order, and with full consideration of the rights of U.S. persons, shall be used to obtain reliable intelligence information to protect the United States and its interests."[39]

The Order aims to promote unity of effort across the IC by charging key officials with responsibility for managing intelligence disciplines: human intelligence (HUMINT), signals intelligence (SIGINT), and geospatial intelligence (GEOINT).[40] Specifically, the Order designates the heads of certain intelligence agencies as the "functional managers" for each discipline: the Director of the CIA for human intelligence, the Director of the NSA for signals intelligence, and the Director of the National Geospatial-Intelligence Agency for geospatial intelligence.[41] Functional managers ensure coordination within and between the IC elements as to the use of those intelligence disciplines.[42] The Order does not define these intelligence disciplines, however, and does not have the effect of neatly segregating the collection activities of the various IC elements.

For example, the authority to collect signals intelligence rests with NSA, subject to specific exceptions. The NSA Director must "[e]stablish and operate an effective unified organization for signals intelligence activities."[43] "No other department or agency may engage in signals intelligence activities except pursuant to a delegation by the Secretary of Defense, after coordination with the Director [of National Intelligence] except for the delegation of operational control over certain operations that are conducted through other elements of the Intelligence Community."[44] (Such an exception has been granted for certain FBI activities.[45])

---

is made available as a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public." *See* CIA Intelligence Activities: Procedures Approved by the Attorney General Pursuant to Exec. Order 12333 § 12.20.

[39] *See* Exec. Order 12333 § 1.1(a). The Order also gives the Director of National Intelligence the authority to designate functional managers for other intelligence disciples. *See id.* at § 1.3(b)(12).

[40] *See id.* at § 1.3(b)(12)(A).

[41] *Id.* at § 1.3(b)(12)(A)(ii), (iii). The Order also gives the Director of National Intelligence freedom to establish other functional managers as needed. *See id.* at § 1.3(b)(12)(A).

[42] Among other things, these functional managers may be called upon to develop policies and procedures relating to their disciplines, ensure coordination across disciplines and agencies, and advise the Director of National Intelligence on "collection capabilities and gaps," "technical architectures," and "processing and dissemination of intelligence." They also play a central role in ensuring that intelligence activities conducted within their disciplines are responsive to priorities established by the President and other top officials.

[43] Exec. Order 12333 §1.7(c)(2); *see also id.* § 1.3(b)(12)(A)(i).

[44] *Id.* at § 1.7(c)(2).

[45] *See* National Security Council Intelligence Directive No. 6. (Feb. 17, 1972), https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/nsa-60th-timeline/1970s/19720217_1970_Doc_3984040_NSCID6.pdf. *See also* "Authorities of the SIGINT Functional Manager"

For human intelligence, by contrast, the Order expressly contemplates that multiple agencies will contribute to the discipline. The Directors of both the CIA and the FBI may "coordinate the clandestine collection of foreign intelligence collected through human sources or through human-enabled means and counterintelligence activities."[46] The CIA coordinates such collection outside the United States, and the FBI coordinates domestic collection. The two agencies also work together on related efforts. For example, if the FBI receives foreign intelligence information from a person in the U.S., the FBI may consult with the CIA regarding the relationship with that person, and the CIA may continue the relationship if the person travels overseas. Other agencies besides the CIA may also engage in human intelligence collection outside the United States.[47]

2. Conduct of Intelligence Activities

Part 2 of the Order describes the need for the collection of foreign intelligence information and the purpose of the Order. Part 2 also establishes "certain general principles that . . . are intended to achieve the proper balance between the acquisition of essential information and protection of individual interests."[48] These principles include the authorization to collect, retain, and disseminate information concerning U.S. person information only in accordance with established procedures; a requirement to use the least intrusive collection technique feasible when inside the United States or directed against a U.S. person abroad; a prohibition on the use of specified intrusive collection techniques except in accordance with established procedures; and authorization to provide assistance to law enforcement and other civil authorities. Part 2 of the Order also addresses other specific intelligence activities.

As noted, the Order requires established procedures for certain intelligence activities. Such procedures are "established by the head of the [IC] element concerned or by the head of a department containing such element and approved by the Attorney General after consultation with the [DNI]."[49] We refer to these procedures throughout this document as an agency's "Attorney General-approved guidelines." Each agency or department has its own guidelines, but these guidelines share some common features. Most guidelines focus on the collection, retention, and dissemination of information concerning U.S. persons. The Attorney General-approved guidelines often supply more detailed rules than the Order itself. Yet they are also written at a high level of generality to accommodate the varied roles of

(Feb. 4, 2013), https://secureservercdn.net/198.71.233.138/q0k.a5d.myftpupload.com/wp-content/uploads/2019/03/Vaughn-index-no-27-02-04-2013-Authorities-of-SIGINT-Functional-Manager2.pdf.

[46] Exec. Order 12333 § 1.3(b)(20)(A)-(B).

[47] *See id.* at § 1.5(i).

[48] *Id.* at § 2.2.

[49] *Id.* at § 2.3.

individual components and different aspects of an IC element's mission. The high level of generality allows for more specific component-level or mission-specific policies, procedures, or guidelines that need not be approved by the Attorney General. Ultimately, those policies, procedures and guidelines must operate in a manner consistent with the Order and the Attorney General-approved guidelines.

Section 2.3 of the Order expressly authorizes the collection, retention, and dissemination of information concerning U.S. persons. However, agencies may only engage in these activities pursuant to Attorney General-approved guidelines. The Order requires that any such guidelines must permit the collection, retention, or dissemination of ten types of information:

1. Publicly available information or information collected with the consent of the person concerned;
2. Foreign intelligence or counterintelligence information, including information concerning corporations or other commercial organizations;
3. Information obtained in the course of lawful foreign intelligence, counterintelligence, international drug, or international terrorism investigations;
4. Information needed to protect the safety of any persons or organizations, including the targets, victims, or hostages of international terrorist organizations;
5. Information needed to protect foreign intelligence or counterintelligence sources, methods, and activities from unauthorized disclosure;
6. Information concerning persons reasonably believed to be potential sources or contacts for the purpose of determining suitability and/or credibility;
7. Information arising out of a lawful personnel, physical, or communications security investigation;
8. Information acquired by overhead reconnaissance not directed at specific U.S. persons;
9. Incidentally obtained information that may indicate involvement in unlawful activities; and
10. Information necessary for administrative purposes.[50]

Section 2.4 of the Order addresses collection techniques. When collecting within the United States or directing collection against U.S. persons abroad, IC elements must use the least intrusive techniques feasible.[51] In addition, the IC may only use more intrusive

[50] *Id.* at § 2.3(a)-(j).

[51] *Id.* at § 2.4.

techniques for lawful governmental purposes in accordance with Attorney General-approved guidelines while protecting constitutional and legal rights.

Moreover, Attorney General-approved guidelines regarding collection techniques may not authorize:

1. The CIA to engage in electronic surveillance within the U.S. except for the purpose of training, testing, or conducting countermeasures to hostile electronic surveillance;
2. Unconsented physical searches in the U.S. by elements of the IC other than the FBI, subject to very limited exceptions;
3. Physical surveillance of a U.S. person in the U.S. by Elements of the IC other than the FBI, with exceptions for IC and military personnel; and
4. Physical surveillance of a U.S. person abroad to collect foreign intelligence, except to obtain significant information that cannot reasonably be acquired by other means.[52]

Section 2.6 of the Order authorizes the IC to provide assistance to law enforcement and other civil authorities. The Order also lays out a number of prohibitions on activities. For example, Section 2.9 prohibits undisclosed participation in any organization in the United States on behalf of the IC element subject to two narrow exceptions. Undisclosed participation may not be for the purpose of influencing the activity of the organization of its members except in accordance with procedures established by the head of the IC element and approved by the Attorney General, after consultation with the DNI. Such undisclosed participation is authorized only if it is essential to achieving lawful purposes. Section 2.10 bans research on human subjects, except in conformance with guidelines issued by the Department of Health and Human Services (HHS). Section 2.11 bans assassination. Section 2.12 forbids an IC element from "participating in or requesting any person to undertake" activities forbidden by the order.

3. General Provisions

Part 3 of the Order contains several general provisions, such as the revocation of preceding executive orders and the definitions of certain terms. It also outlines the role of Congress in overseeing the implementation of the Order and provides a framework for resolving certain disputes.

C. The Broader Legal Context

Intelligence collection governed by the Order may be subject to other requirements enshrined in statute or required by Executive Branch policy. One example is FISA, a statute

[52] *Id.*

that imposes certain requirements on the surveillance of individuals in the United States and U.S. persons abroad.

For example, Section 2.5 of the Order allows the Attorney General to approve the use of an intelligence collection technique against a person within the United States or against a U.S. person abroad, even if that technique would require a warrant if undertaken for law enforcement purposes. FISA, however, requires a court-issued order for many foreign intelligence wiretaps and physical searches in the United States (and, if they target a U.S. person, overseas).[53]

PPD-28 also limits how agencies can exercise authorities conferred by the Order. Issued in 2014, PPD-28 establishes by presidential directive various limitations on U.S. signals intelligence activities. For example, PPD-28 limits the use of "signals intelligence collected in bulk" and requires signals intelligence activities to include "appropriate safeguards" for the personal information of all individuals, regardless of nationality or place of residence. PPD-28 remains in effect and is binding within the IC.

III. Frequently Asked Questions

Given the breadth of topics and issues included in the Board's EO 12333 review, as well as stakeholder interest in this review, this section answers some frequently asked questions.

1. Does EO 12333 authorize agencies to conduct searches and surveillance inside the United States targeting U. S. persons?

Yes, in limited circumstances.[54] Section 2.4 of the Order forbids the unconsented physical search or electronic surveillance of a U.S. person within the territorial United States, except: (1) searches or surveillance by the Federal Bureau of Investigation; (2) searches by counterintelligence elements of the military, directed against U.S. military personnel, for intelligence purposes and based on a finding of probable cause that the target is acting as an agent of a foreign power; (3) physical surveillance of present or former employees, contractors, or applicants of IC elements; and (4) physical surveillance of a military person employed by a nonintelligence element of a military service. If, however, a statute like FISA imposes additional requirements on the activity—for example, requiring a FISA warrant to conduct physical search or electronic surveillance of a U.S. person—the agency must comply with the more stringent statutory requirements.

To engage in any of these activities, the IC must use the least intrusive techniques feasible. Some techniques that are considered particularly intrusive, such as using a monitoring

[53] Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 *et. seq.*

[54] See Sec. II.B.2 above.

device,[55] may only be used in conformance with an agency's Attorney General-approved guidelines.[56]

2. Does EO 12333 prohibit agencies from collecting intelligence targeting U. S. persons outside the United States?

No, but it imposes certain restrictions.[57] Section 2.5 of EO 12333 requires Attorney General approval to use "any technique for which a warrant would be required if undertaken for law enforcement purposes" against U.S. persons abroad for intelligence purposes. The Attorney General's approval must be based on a determination that probable cause exists to believe the U.S. person is a foreign power or an agent of a foreign power. Section 2.4 of EO 12333 also imposes restrictions on the techniques that may be used for collection. Further, FISA may impose additional requirements on such activities in some cases.[58]

3. Under EO 12333, can IC employees investigate whatever they want?

No. The Order requires IC efforts to be responsive to specific needs for information conveyed by the President and top executive branch policymakers. As such, it is intended to ensure that intelligence agencies and their employees cannot simply decide for themselves what to collect.

The primary way in which the Executive Branch establishes intelligence priorities and communicates them to the IC is through the National Intelligence Priorities Framework.[59] The National Intelligence Priorities Framework is a classified document containing topics that have been identified as intelligence priorities through a formal system led by the DNI. All intelligence that the IC collects must be responsive to one of these listed priorities. This requirement helps ensure that the IC follows the Order's directive to collect information and

---

[55] *See* Exec. Order 12333 § 2.4 ("Agencies are not authorized to use such techniques as electronic surveillance, unconsented physical search, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the agency concerned and approved by the Attorney General.").

[56] *See id.*

[57] See Sec. II.B.2 above.

[58] *See* 50 U.S.C. § 1881(c), (d). Sections 704 and 705(b) of FISA build upon these requirements in Section 2.5 of the Order and provide that, in addition to the Attorney General's approval, the government must obtain an order from the Foreign Intelligence Surveillance Court ("FISC") in situations where the U.S. person target has "a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted inside the United States for law enforcement purposes." The FISC order must be based upon a finding that there is probable cause to believe that the target is a foreign power, an agent of a foreign power, or an officer or employee of a foreign power and that the target is reasonably believed to be located outside the United States.

[59] *See* Intelligence Community Directive No. 204, National Intelligence Priorities Framework §§ B.1, D.1 (Jan. 2, 2015), https://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligence%20Priorities%20Framework.pdf.

conduct activities regarding national security threats in accordance with the President's priorities.[60]

4. How does EO 12333 limit the ways in which the IC may act to influence domestic public opinion?

The Order forbids the IC from attempting to influence American politics, opinion, media, activism, and academia through covert action. Specifically, the Order states that "[n]o covert action may be conducted which is intended to influence United States political processes, public opinion, policies, or media,"[61] regardless of whether the action is taken inside or outside the United States.[62] For example, EO 12333 would not allow an IC element to take covert actions intended to persuade voters to elect a particular candidate.

Further, the Order states that "[n]o one acting on behalf of elements of the Intelligence Community may join or otherwise participate in any organization in the United States on behalf of any element of the Intelligence Community without disclosing such person's intelligence affiliation," except where the activity is conducted "in accordance with procedures established by the head of the Intelligence Community element concerned or the head of a department containing such element and approved by the Attorney General, after consultation with the [DNI]."[63] For example, under the CIA's Attorney General-approved guidelines "a CIA officer who had not disclosed their affiliation could not propose a new policy for the organization, suggest a new course of action, attempt to convince members to modify an established practice, or otherwise in any way attempt to influence the activities of the organization."[64] Whether a person acting on behalf of an IC element may participate in a U.S. organization without disclosing his or her intelligence affiliation is, however, complex and fact-dependent.[65]

---

[60] *See* Exec. Order. 12333 § 1.4(a)-(b).

[61] *See id.* at § 2.13.

[62] *See id.* at § 2.13.

[63] *See id.* at § 2.9. An exception applies when the participation is undertaken on behalf of the FBI in the course of a lawful investigation or when the organization in question is composed primarily of individuals who are not U.S. persons and is reasonably believed to be acting on behalf of a foreign power.

[64] *See* CIA, The CIA's Updated Executive Order 12333 Attorney General Guidelines, 8 (last visited Oct. 12, 2020), https://www.cia.gov/about-cia/privacy-and-civil-liberties/Detailed-Overview-CIA-AG-Guidelines.pdf. ("CIA Guidelines Overview") (commenting on § 9.3.2(g) of CIA's Attorney General Guidelines).

[65] In addition, IC elements' guidelines also prohibit employees and contractors from taking action related to a U.S. person based solely on activities by the U.S. person that are protected under the First Amendment. *See, e.g.*, CIA Attorney General-approved Guidelines § 3.3 ("CIA is not authorized to and shall not collect or maintain information concerning U.S. persons solely for the purpose of monitoring (1) activities protected by the First Amendment . . . ."); Department of Defense Manual 5240.01, Procedures Governing the Conduct of DoD Intelligence Activities § 1.2(b)(3) ("DoD Components . . . [m]ay not investigate U.S. persons or collect or maintain information about them solely for the purpose of monitoring

5. Does EO 12333 ban any activities outright?

Yes, the Order bans some activities outright. No intelligence agency may participate in assassinations. No intelligence agency may conduct human experimentation, except in conformance with broadly applicable HHS guidelines. No intelligence agency may conduct covert action intended to influence United States political processes, public opinion, policies, or media. Moreover, the Order forbids an element of the IC from participating in or requesting any person to undertake activities forbidden by the Order.

6. What oversight is there of the IC's use of EO 12333?

A variety of entities both inside and outside of the IC conduct oversight. In Congress, the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence oversee EO 12333 activities to ensure consistency with law, regulation, and, increasingly, policy considerations relating to privacy and civil liberties. Intelligence agencies must keep the Congressional intelligence committees "fully and currently informed" of all intelligence activities.[66]

There are several oversight entities within the executive branch as well. These include the Attorney General, who approves the guidelines that regulate agencies' activities under the Order. The President's Intelligence Advisory Board provides advice to the President concerning the quality and adequacy of intelligence collection, analysis, counterintelligence, and other intelligence activities.[67] The Intelligence Oversight Board, a standing committee of the President's Intelligence Advisory Board, oversees the IC's compliance with the Constitution, statutes, and executive orders.[68] And various Inspectors General and privacy and civil liberties officers review activities to ensure compliance with law and policy. Additionally, the Privacy and Civil Liberties Oversight Board conducts oversight reviews and provides advice that is, in both cases, related to efforts to protect the nation against terrorism.

---

activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States."); Attorney General's Guidelines for Domestic FBI Operations § I(C)(3) ("These Guidelines do not authorize investigating or collecting or maintaining information on United States persons solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States."); National Counterterrorism Center Attorney General-approved Guidelines § III(a)(4) ("NCTC shall not access, acquire, retain, use, or disseminate United States person information solely for the purpose of monitoring activities protected by the First Amendment or monitoring the lawful exercise of other rights secured by the Constitution or other laws of the United States."). For example, the CIA "could not collect the public statement of or about a United States person merely because he or she was making critical statements regarding the United States government." CIA Guidelines Overview at 3.

[66] *See* 50 U.S.C. § 3091.

[67] *See* Exec. Order 10656.

[68] *See* Exec. Order 13462.

7. Can intelligence agencies share information collected under EO 12333 with federal law enforcement authorities?

Yes. The Order permits intelligence agencies to share information with federal law enforcement under certain circumstances and requires the IC elements to report possible violations of federal criminal laws by the element's employees or in accordance with the element's Attorney General-approved guidelines.[69]

EO 12333 does not generally prohibit sharing information with law enforcement. Rather, it permits the IC to engage in specific activities, such as cooperating in law enforcement activities to investigate or prevent clandestine intelligence activities by foreign powers, or international terrorist or narcotics activities.[70] And it generally allows the IC to provide "other assistance and cooperation to law enforcement" that is not prohibited by law.[71]

The Order also expressly permits IC agencies to collect, retain, or disseminate incidentally obtained information about a United States person if the information "may indicate involvement in activities that may violate Federal, state, local, or foreign laws."[72]

Further, the heads of the IC elements are required to "[r]eport to the Attorney General possible violations of criminal laws by employees[.]"[73] They must also report to the Attorney General violations "of specified Federal criminal laws by any other person" in a manner consistent with the protection of intelligence sources and methods and subject to certain procedures.[74] The specified criminal laws are agreed upon by the Attorney General and the head of the IC element.[75] So, for example, if in the course of collecting foreign intelligence information about an adversarial foreign government leader, an intelligence agency learned that a U.S. citizen were engaging in trafficking controlled munitions or technology to the foreign government, the intelligence agency must report that information to the Department of Justice as a potential violation of federal criminal law.

---

[69] *See* Exec. Order 12333 §§ 1.6(b), 2.3(i).

[70] *Id.* at § 2.6(a).

[71] *Id.* at § 2.6(d).

[72] *Id.* at § 2.3(i).

[73] *Id.* at § 1.6(b).

[74] *Id.*

[75] *Id.* The referenced procedures are set forth in a Memorandum of Understanding between each IC element and the Attorney General, except for the intelligence elements of the FBI and the Department of Treasury. Memorandum of Understanding: Reporting of Information Concerning Federal Crimes between the Attorney General; Secretary of Defense; Director of the CIA; Director of the NSA; Director of the Defense Intelligence; Assistant Secretary of State, Intelligence and Research; and the Director of the Office of Non-Proliferation and National Security, Department of Energy (last signed Aug. 22, 1995).

8. How else does EO 12333 allow the IC to assist federal law enforcement?

EO 12333 permits intelligence agencies to assist federal law enforcement by providing "specialized equipment, technical knowledge, or assistance of expert personnel."[76] The Order also provides for such assistance to support local law enforcement agencies "when lives are endangered."[77] The General Counsel of an IC element must approve the use of its expert personnel by a law enforcement entity.[78]

9. Who receives protections under EO 12333?

The Order's protections are focused on activities that implicate U.S. persons or are conducted in the United States.[79] Yet this is not to say that foreign citizens receive no benefit from EO 12333. When non-U.S. persons are in the United States, they are protected by certain rules that apply within the United States regardless of a person's nationality.[80] And more generally, those aspects of the Order that require agency personnel to focus on legitimate intelligence goals protect all persons. In addition, a separate presidential policy directive, PPD-28, seeks expressly to safeguard personal information collected through signals intelligence regardless of nationality.[81]

---

[76] *Id.* at § 2.6(c).

[77] *Id.*

[78] *Id.*

[79] *See id.* at §§ 2.3, 2.4, 2.5.

[80] *See id.* at § 2.4 (limiting collection techniques with regard to information collected within the United States, regardless of nationality of target); *id.* at § 2.5 (stating Attorney General approval necessary for collection within the United States for which a warrant would be required if undertaken for law enforcement purposes). Further, many of the protections regarding unevaluated information, which must be handled according to Attorney General-approved guidelines, result in protections for both non-United States person and United States persons.

[81] *See* Privacy and Civil Liberties Oversight Board, *Report to the President on the Implementation of Presidential Policy Directive 28: Signals Intelligence Activities* (Oct. 16, 2018), https://documents.pclob.gov/prod/Documents/OversightReport/16f31ea4-3536-43d6-ba51-b19f99c86589/PPD-28%20Report%20(for%20FOIA%20Release).pdf.