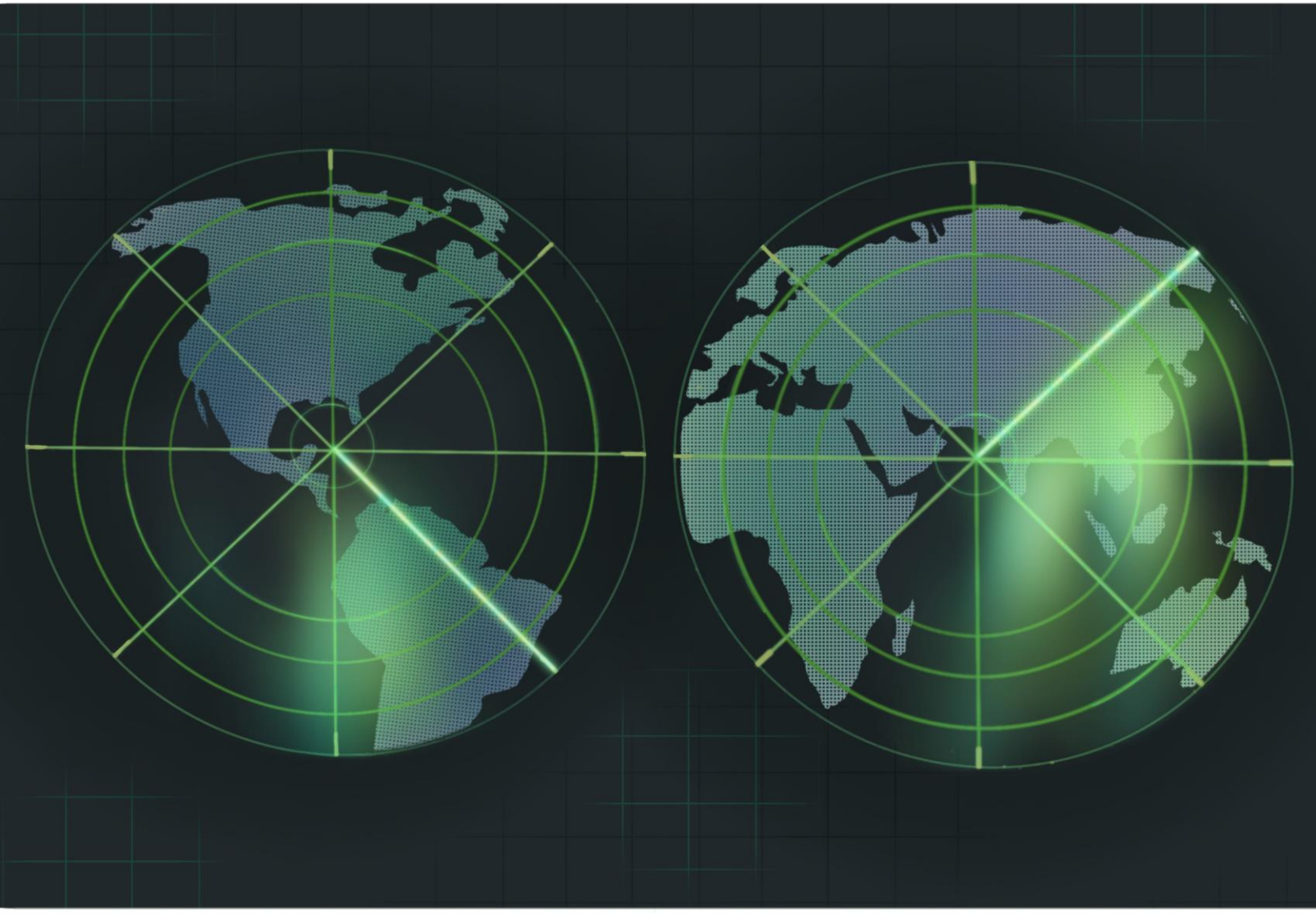
The Privacy and Civil Liberties Oversight Board



Review of Policies and Procedures Implementing Enhanced Safeguards for U.S. Signals Intelligence Activities

Staff Report

September 25, 2025

[THIS PAGE INTENTIONALLY LEFT BLANK]

THE
PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

REVIEW OF POLICIES AND PROCEDURES IMPLEMENTING ENHANCED SAFEGUARDS FOR U.S. SIGNALS INTELLIGENCE ACTIVITIES

STAFF REPORT

SEPTEMBER 25, 2025

Privacy and Civil Liberties Oversight Board

Beth A. Williams, Board Member

PCLOB acknowledges with gratitude the staff members who worked on this project, including Cameron Brown, Hannah Burgess, Jennifer Fitzpatrick, Ryan Fletcher, Laura Grasso, David Husband, Tatjana Naquin, Alexa Potter, Alan Silverleib, Courtney Sullivan, and other current and former staff members.

STATEMENT FROM BOARD MEMBER BETH A. WILLIAMS

This report by the staff of the Privacy and Civil Liberties Oversight Board ("PCLOB") fulfills PCLOB's commitment to "conduct a review of the updated policies and procedures" implemented by elements of the U.S. Intelligence Community ("IC") to comply with Executive Order ("E.O.") 14086, *Enhancing Safeguards for United States Signals Intelligence Activities* ("the Executive Order").

As described in detail in the following pages, PCLOB has found that all IC elements' updated policies and procedures, as required under E.O. 14086, align the rules for handling of non-U.S. persons' personal information collected through signals intelligence activities with the rules for handling of U.S. persons' personal information collected through signals intelligence activities. PCLOB has assessed that all IC elements have implemented policies and procedures that ensure compliance with the Executive Order's safeguards for collection, use, retention, and dissemination of information collected by IC elements' signals intelligence activities. PCLOB has also assessed that those policies and procedures provide for the requisite documentation of signals intelligence activities, training of personnel on the requirements of the enhanced safeguards established by the Executive Order, and oversight of IC personnel's compliance with those requirements.

The report makes two recommendations for improvement in the protections for privacy and civil liberties by IC elements: (1) for each element to require regular training of its personnel; and (2) for each element to make available to the public, consistent with the protection of national security, any further updates or changes to its policies and procedures.

I endorse the report in its entirety. The professional staff's review of the IC elements' updated policies and procedures was comprehensive, and their assessments and recommendations are well-founded and reasonable. I commend the professionalism and appreciate the diligent work of the PCLOB staff. This report provides important transparency regarding the U.S. government's policies and procedures concerning its signals intelligence activities, and I am confident that it will contribute significantly to the public discourse on those activities both in the United States and abroad.

Beth A. Williams
Board Member
September 25, 2025

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Executive Order 14086, *Enhancing Safeguards for United States Signals Intelligence Activities* (E.O. 14086 or the Executive Order), issued in October 2022, establishes government-wide safeguards for U.S. signals intelligence activities consistent with the protection of privacy and civil liberties for all persons, regardless of nationality or place of residence. The Executive Order requires the head of each Intelligence Community (IC) element to update its policies and procedures that had been issued pursuant to the 2014 Presidential Policy Directive 28 (PPD-28), *Signals Intelligence Activities*, to implement the Executive Order's enhanced privacy and civil liberties safeguards and to release the updated policies and procedures publicly "to the maximum extent possible."[1]

IC elements have *complied with the requirements* of the Executive Order by implementing policies and procedures consistent with the expanded privacy and civil liberties protections therein.

The Privacy and Civil Liberties Oversight Board staff (PCLOB) issues this report[2] in accordance with the Executive Order, which encourages the Privacy and Civil Liberties Oversight Board to review the updated policies and procedures to ensure they are consistent with the Executive Order's enhanced safeguards.[3] PCLOB finds that the IC elements have complied with the requirements of the Executive Order by implementing policies and procedures consistent with the expanded privacy and civil liberties protections therein. Some policies and procedures are new, drafted since the issuance of the Executive Order, while others present updates to, or reaffirmations of, older documents imposing requirements that are the same as or similar to Executive Order requirements. In the event that IC elements update or change their implementing policies and procedures,

[1] Proclamation No. 14086, 87 Fed. Reg. 62283, § 2(c)(iv)(A)-(C) (Oct. 14, 2022), https://www.federalregister.gov/documents/2022/10/14/2022-22531/enhancing-safeguards-for-united-states-signals-intelligence-activities [hereinafter E.O. 14086].

[2] Board Member Williams and PCLOB staff thank the IC, and especially the Office of the Director of National Intelligence's (ODNI) Office of Civil Liberties, Privacy, and Transparency (CLPT), for its cooperation and assistance with PCLOB's questions and requests during the preparation of this report.

[3] The initiation of this oversight project was approved by a quorate Board in 2023. The report contains the analysis of PCLOB's staff but has not been voted on or approved by a quorate Board. Per PCLOB's Sub-Quorum Policy, adopted October 23, 2024, all conditions for publication of this report have been met. *See* Priv. and C.L. Oversight Bd., *Sub-Quorum Authorities and Operations when Position of Chair is Vacant*, Policy 102-01, at § 6.1.C (2024), https://documents.pclob.gov/prod/DynamicImages/Generic/59b039ee-73ef-44fc-a80d-862d10a2ca84/102-01~1.PDF.

PCLOB recommends that they make those updated versions publicly available to the maximum extent practicable consistent with the protection of national security.

PCLOB finds that all IC elements' policies and procedures, as required under E.O. 14086, align the rules for handling of non-U.S. persons' personal information collected through signals intelligence activities with the rules for handling of U.S. persons' personal information collected through signals intelligence activities. Due to the additional obligations and privacy risks associated with collecting raw signals intelligence, or other information subject to E.O. 14086, the IC elements that collect such intelligence—the Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), and National Security Agency (NSA)—have more extensive policies and procedures compared to other IC elements. PCLOB also finds that each IC element that collects signals intelligence has in place senior-level legal, oversight, and compliance officials who oversee signals intelligence activities, as required under the Executive Order.

Based on the information available to PCLOB as of the date of this report, no IC element has to date experienced a significant incident of non-compliance with the Executive Order. Training IC personnel on Executive Order requirements and IC elements' policies and procedures remains important to ensure future compliance, however. While PCLOB finds that the IC elements have implemented training requirements to ensure that all personnel with access to signals intelligence or other information subject to E.O. 14086 abide by the Executive Order's requirements, we recommend that IC elements require regular trainings on E.O. 14086 to ensure that personnel are informed of any legal, policy, or procedural updates.

PCLOB assesses that all IC elements reviewed have implemented sufficient internal processes to ensure compliance, review, and oversight of signals intelligence activities conducted by their personnel.

I. INTRODUCTION

E.O. 14086 memorializes the importance of signals intelligence activities to the national security of the United States, while concurrently building upon existing policy to ensure that in the planning and execution of signals intelligence activities, there is appropriate consideration of the protection of the privacy and civil liberties of all persons, regardless of nationality or place of residence.[4] The Executive Order states:

> The United States collects signals intelligence so that its national security decisionmakers have access to the timely, accurate, and insightful information necessary to advance the national security interests of the United States and to protect its citizens and the citizens of its allies and partners from harm . . . . At the same time, the United States recognizes that signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information.[5]

While the Executive Order does not define "signals intelligence," and the term is not uniformly defined across the IC, NSA defines signals intelligence as "intelligence derived from electronic signals and systems used by foreign targets, such as communications systems, radars, and weapons systems that provides a vital window for our nation into foreign adversaries' capabilities, actions, and intentions."[6] IC elements apply E.O. 14086 to their signals intelligence activities, including those authorized under Executive Order

[4] E.O. 14086 is divided into five sections. Section 2, *Signals Intelligence Activity*, is most relevant here and portions of that section are discussed in this report. This report does not analyze all sections of the Executive Order in detail. Section 1 sets forth the "purpose" of E.O. 14086 (to advance and uphold U.S. national security interests while recognizing that signals intelligence activities must take into account that all persons have legitimate privacy interests in the handling of their personal information); Section 3 creates a redress mechanism for binding review of qualifying complaints; Section 4 contains definitions; and Section 5 provides a general description of how the Executive Order interacts with other legal authorities and other legal limitations and rights.

[5] E.O. 14086 § 1.

[6] Nat'l Sec. Agency, *Signals Intelligence (SIGINT) Overview*, https://nsa.gov/Signals-Intelligence/Overview (last visited Sept. 22, 2025).

12333[7] (E.O. 12333) and Section 702 of the Foreign Intelligence Surveillance Act (FISA).[8]

The Executive Order requires the heads of each IC element[9] to update their policies and procedures that were issued pursuant to PPD-28 as necessary to implement the Executive Order's enhanced privacy and civil liberties safeguards and to release the updated policies and procedures publicly "to the maximum extent possible."[10] In updating their policies and procedures, IC elements are required to consult with PCLOB, the Attorney General, and the Civil Liberties Protection Officer (CLPO) of the ODNI. PCLOB provided advice to the IC elements on the drafting of their respective policies and procedures on April 20, 2023. In July 2023, ODNI publicly released the IC elements' updated policies and procedures.[11]

---

[7] E.O. 12333 is a foundational document for the United States' foreign intelligence efforts. It establishes a framework that applies broadly to the government's collection, analysis, and use of foreign intelligence and counterintelligence, authorizes various forms of collection, constructs administrative and oversight infrastructure, and outlines protections for U.S. persons. It requires all IC elements to develop guidelines approved by the Attorney General governing the collection, retention, and dissemination of information concerning U.S. persons. Exec. Order No. 12,333, 3 C.F.R. §§ 2.3, 3.4 (1981); *see* Priv. and C.L. Oversight Bd., *Executive Order 12333*, at 4 (2021), https://documents.pclob.gov/prod/Documents/OversightReport/b11b78e0-019f-44b9-ae4f-60e7eebe8173/12333%20Public%20Capstone.pdf.

[8] FISA Section 702 permits the Attorney General and the Director of National Intelligence (DNI) to jointly authorize surveillance conducted using the compelled assistance of U.S. electronic communications surveillance providers to target non-U.S. persons, reasonably believed to be located outside of the United States, for the purpose of collecting foreign intelligence information. 50 U.S.C. § 1881a; *see generally* Priv. and C.L. Oversight Bd., *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (2023), https://documents.pclob.gov/prod/Documents/OversightReport/e9e72454-4156-49b9-961a-855706216063/2023%20PCLOB%20702%20Report%20(002).pdf [hereinafter 2023 PCLOB Section 702 Report].

[9] The IC elements are as follows:

- ODNI,
- CIA,
- The Department of Energy Office of Intelligence and Counterintelligence (DOE-IN),
- The Department of State Bureau of Intelligence and Research (State INR),
- The Department of Treasury Office of Intelligence and Analysis (Treasury OIA),
- Within the Department of Defense (DoD), the Defense Intelligence Agency (DIA), the National Geospatial Intelligence Agency (NGA), the National Reconnaissance Office (NRO), NSA, and the intelligence elements of the five DoD armed services—the Army, Navy, Marine Corps, Air Force, and Space Force,
- Within the Department of Homeland Security (DHS), the DHS Office of Intelligence and Analysis (DHS I&A) and the U.S. Coast Guard (DHS USCG), and
- Within the Department of Justice (DOJ), the Drug Enforcement Administration Office of National Security Intelligence (DEA ONSI) and FBI.

[10] E.O. 14086 § 2(c)(iv)(A)-(C).

[11] Off. of the Dir. of Nat'l Intel., *ODNI Releases Intelligence Community Procedures Implementing New Safeguards in Executive Order 14086* (July 3, 2023), https://www.intelligence.gov/ic-on-the-record-

PCLOB issues this report in accordance with the Executive Order, which encourages PCLOB to review the updated policies and procedures to ensure they are consistent with the Executive Order's enhanced safeguards, and consistent with PCLOB's mission to "continually review . . . the regulations, policies, and procedures, and the implementation of the regulations, policies, and procedures, of the departments, agencies, and elements of the executive branch relating to efforts to protect the Nation from terrorism to ensure that privacy and civil liberties are protected."[12] In conducting its review, PCLOB received both classified and unclassified materials from the IC elements. Consistent with PCLOB's mission and in the interest of transparency, PCLOB is publishing this report in an unclassified form. The Executive Order mandates that, within 180 days of the completion of this review, the head of each IC element "shall carefully consider and implement or otherwise address all recommendations contained in PCLOB's review, consistent with applicable law."[13]

In conducting its review, PCLOB examined all IC elements' E.O. 14086 policies and procedures, supplemental guidance (where relevant), and training materials. This report focuses largely on the implementation of the Executive Order by NSA, CIA, and FBI because those agencies alone collect signals intelligence, or information that they consider to be covered by E.O. 14086, and possess or handle unevaluated signals intelligence. This report highlights key aspects of IC elements' policies and procedures and explains where differences emerge in the implementation of the Executive Order. This report does not include a review of the processing of qualifying complaints under the redress mechanism established by E.O. 14086. PCLOB intends for that topic to be addressed in a future report.

database/results/oversight/odni-releases-ic-procedures-implementing-new-safeguards-in-executive-order-14086.

[12] 42 U.S.C. § 2000ee(d)(2)(A); *see* E.O. 14086 § 2(c)(v)(A). PCLOB previously consulted with the Attorney General on appointment of members to the Data Protection Review Court established by the Executive Order and advised IC elements on revisions to their governing Attorney General Guidelines in order to comply with the Executive Order. *See* E.O. 14086 §§ (2)(a)(iv)(B), 3(d)(i)(A).

[13] E.O. 14086 § 2(c)(v)(B).

II. BACKGROUND

A. Presidential Policy Directive 28

PPD-28, issued on January 17, 2014, was the first policy document in which the U.S. government publicly articulated the limitations on the use of signals intelligence collected in bulk, refined the process for collecting signals intelligence, and extended to foreign nationals certain privacy protections as to their personal information that were previously afforded only to U.S. persons.[14] It recognized both that the collection of signals intelligence "is necessary for the United States to advance its national security and foreign policy interests and to protect its citizens and the citizens of its allies and partners from harm," and that all persons have "legitimate privacy interests in the handling of their personal information, regardless of their nationality or wherever they might reside."[15]

PPD-28 refined the process for collecting signals intelligence in light of the unique nature of such collection and the risks entailed in conducting these activities.[16] It states:

> [S]ignals intelligence collection raises special concerns, given the opportunities and risks created by the constantly evolving technological and geopolitical environment, the inherent concerns raised when signals intelligence can be collected in bulk, and the risk of damage to our national security interests and our law enforcement, intelligence-sharing, and diplomatic relationships should our capabilities or activities be compromised.[17]

Further, PPD-28 directed the heads of departments and agencies that participate in the policy processes for establishing signals intelligence priorities and requirements to review annually any priorities or requirements identified by their departments or agencies and

[14] *See generally* Presidential Policy Directive/PPD-28, 1 PUB. PAPERS 46, at § 2-4 (Jan. 17, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities [hereinafter PPD-28]. PCLOB reviewed the policies and procedures that IC elements adopted to implement PPD-28 in a 2018 oversight report. *See* Priv. and C.L. Oversight Bd., *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/caec5956-e1e4-4d11-a840-6e13114962c1/PPD-28%20Report%20(for%20FOIA%20Release)%20-%20Completed%20508%20-%2012082022.pdf.

[15] PPD-28, *supra*, at § 2.

[16] *Id*. at § 3.

[17] *Id.* E.O. 14086 § 4(b) defines "bulk collection" as "the authorized collection of large quantities of signals intelligence data that, due to technical or operational considerations, is acquired without the use of discriminants (for example, without the use of specific identifiers or selection terms)." E.O. 14086 § 4(b).

advise the Director of National Intelligence (DNI) whether each should be maintained.[18] PPD-28 affirmed "that determinations about whether and how to conduct signals intelligence activities must carefully evaluate the benefits to our national interests and the risks posed by those activities."[19]

B. Executive Order 14086

E.O. 14086 memorializes and builds upon PPD-28's principles, safeguards, and requirements by, among other things, incorporating the principles of "necessity" and "proportionality" in the conduct of signals intelligence activities; denoting twelve "legitimate objectives" for which signals intelligence can be collected and four "prohibited" objectives for which it cannot; directing that the ODNI CLPO participate in assessing signals intelligence collection priorities; requiring that the retention and dissemination standards for personal information collected through signals intelligence for non-U.S. persons generally align with those for U.S. persons; and imposing new training and oversight obligations.[20]

Upon the issuance of E.O. 14086, the President circulated National Security Memorandum 14 (NSM-14) to the heads of all IC elements. NSM-14 revoked all provisions of PPD-28 except Section 3, Section 6, and its Classified Annex, deeming the provisions "essential to maintain the policy process refined by [these sections], under which national security policymakers consider carefully the value of signals intelligence activities to our national interests and the risks entailed in conducting those activities."[21] E.O. 14086 directed the IC elements to

[18] PPD-28, *supra,* at § 3. Under the National Security Act of 1947, as amended by the Intelligence Reform and Terrorism Prevention Act of 2004, the DNI is obligated to establish objectives for the collection, analysis, production, and dissemination of national intelligence and ensure that timely and objective national intelligence is provided to the President. The DNI was further directed to "establish and manage a robust National Intelligence Priorities Framework . . . process which responds to the [President's Intelligence Priorities] and ensures that both the IC and additional departments and agencies that require intelligence are represented in the process of developing priorities." *Id*. at § 2(c).

[19] *Id*. at § 3.

[20] *See generally* E.O. 14086.

[21] National Security Memorandum on Partial Revocation of Presidential Policy Directive 28/NSM-14, 8 WEEKLY COMP. PRES. DOC. 1 (Oct. 7, 2022), https://www.govinfo.gov/content/pkg/DCPD-202200895/pdf/DCPD-202200895.pdf. The revoked sections of PPD-28 were as follows: Section 1 articulated four "principles" with which signals intelligence collection must be consistent, including that privacy and civil liberties shall be integral considerations in the planning of U.S. signals intelligence activities; Section 2 put in place a set of six limitations on the use of signals intelligence collected in bulk, which were essentially retained by E.O. 14086; Section 4 required the DNI, in consultation with the Attorney General, to ensure that all IC elements establish policies and procedures that provide certain safeguards for information of all persons, regardless of nationality, when it is collected through signals intelligence activities; Section 5 required the DNI to provide a "status report" on the progress of PPD-28's implementation and encouraged PCLOB to provide the President with a report assessing the directive's implementation. *See* PPD-28, *supra*, at §§ 1-2, 4-5.

continue to use their existing policies and procedures issued under PPD-28 until they could update them to conform to the requirements of the Executive Order.[22] ODNI publicly released the IC elements' updated policies and procedures in July 2023.[23] This report examines those implementing policies and procedures.

1. Principles

Section 2 of the Executive Order sets forth three "principles" that govern the conduct of signals intelligence activities. First, such activities shall be "subject to appropriate safeguards, which shall ensure that privacy and civil liberties are integral considerations in the planning and implementation of such activities."[24] These safeguards include requirements that signals intelligence activities be "necessary to advance a validated intelligence priority"[25] and be "conducted only to the extent and in a manner that is proportionate to the validated intelligence priority for which they have been authorized."[26]

---

[22] E.O. 14086 § 2(c)(iv). Unlike in response to PPD-28, ODNI did not establish a working group or issue a status report on the IC's implementation of E.O. 14086 while agencies were updating policies to comply with it in the first few years after its issuance. However, all relevant policies and procedures were updated as of July 3, 2023.

[23] *ODNI Releases Intelligence Community Procedures Implementing New Safeguards in Executive Order 14086*, *supra.*

[24] E.O. 14086 § 2(a)(ii).

[25] Section 4(n) defines "validated intelligence priority" as follows:

> [F]or most United States signals intelligence collection activities, a priority validated under the process described in section 2(b)(iii) of this order; or, in narrower circumstances (for example when such process cannot be carried out because of a need to address a new or evolving intelligence requirement), shall mean a priority set by the President of the head of an element of the [IC] in accordance with criteria described in section 2(b)(A)(1)-(3) of this order to the extent feasible.

Id. § 4(n).

[26] According to E.O. 14086 § 2(a)(ii)(A)-(B):

> Signals intelligence activities shall be subject to appropriate safeguards, which shall ensure that privacy and civil liberties are integral considerations in the planning and implementation of such activities so that:
>
> (a) signals intelligence activities shall be conducted only following a determination, based on a reasonable assessment of all relevant factors, that the activities are necessary to advance a validated intelligence priority, although signals intelligence does not have to be the sole means available or used for advancing aspects of the validated intelligence priority; and
>
> (b) signals intelligence activities shall be conducted only to the extent and in a manner that is proportionate to the validated intelligence priority for which they have been authorized, with the aim of achieving a proper balance between the importance of the validated intelligence priority being advanced and the impact on privacy and civil liberties of all persons, regardless of their nationality and where ever they might reside.

Second, such activities must be "authorized by statute or Executive Order, proclamation, or other Presidential directive and undertaken in accordance with the Constitution and applicable statutes and Executive Orders, proclamations, and other Presidential directives."[27] Third, such activities must be subject to "rigorous oversight."[28]

2. Objectives

The Executive Order further provides that signals intelligence activities shall be conducted only in pursuit of one or more of the following twelve legitimate objectives:

1. understanding or assessing foreign government capabilities, intentions, or activities;
2. understanding or assessing foreign organizations that pose a current or potential threat;
3. understanding or assessing transnational threats that impact global security;
4. protecting against foreign military capabilities or activities;
5. protecting against foreign terrorism or the taking of hostages by or on behalf of a foreign government, foreign organization, or foreign person;
6. protecting against foreign espionage, sabotage, assassination, or other intelligence activities;
7. protecting against foreign threats from weapons of mass destruction;
8. protecting against foreign cyber threats;
9. protecting against threats to U.S., allied, or partner personnel;
10. protecting against transnational criminal threats;
11. protecting election integrity and U.S. infrastructure from foreign activities; and
12. advancing collection or operational capabilities or activities to further a legitimate objective.[29]

In addition to these twelve objectives, the President may authorize updates to the list of objectives in light of new national security imperatives, such as "new or heightened threats" to national security.[30] The DNI is required to publicly release any updates to the list, unless doing so would pose a risk to national security.[31]

Id. § 2(a)(ii)(A)-(B).

[27] *Id.* § 2(a)(i).

[28] *Id.* § 2(a)(iii).

[29] *Id.* § 2(b)(i)(A).

[30] *Id.* § 2(b)(i)(B).

[31] *Id.*

The Executive Order also explicitly prohibits four objectives, stating that signals intelligence shall not be conducted for the purpose of:

1. suppressing or burdening criticism, dissent, or the free expression of ideas or political opinions by individuals or the press;
2. suppressing or restricting legitimate privacy interests;
3. suppressing or restricting a right to legal counsel; or
4. disadvantaging persons based on their ethnicity, race, gender, gender identity, sexual orientation, or religion.[32]

In addition, the Executive Order states that it is not a legitimate objective "to collect foreign private commercial information or trade secrets to afford a competitive advantage" to U.S. companies and business sectors commercially.[33] However, the collection of such information is authorized to protect the national security of the United States or its allies or partners.[34]

3. Validation of Collection Priorities

The Executive Order expands the role of the ODNI CLPO in the National Intelligence Priorities Framework (NIPF) process.[35] The DNI is required to obtain from the ODNI CLPO an assessment as to whether each of the intelligence priorities identified in the NIPF advance one or more of the twelve legitimate objectives; was neither designed nor anticipated to result in signals intelligence in contravention of the four prohibited objectives; and "was established after appropriate consideration of the privacy interests of all persons, regardless of their nationality or wherever they might reside."[36] If the DNI disagrees with any portion of the ODNI CLPO's assessment, the DNI must include the ODNI CLPO's assessment and the DNI's views when presenting the NIPF to the President.[37] ODNI reported that there have

[32] *Id*. § 2(b)(ii)(A). While executive branch policy is to use the word "sex" in place of "gender," and that "gender identity" "does not provide a meaningful basis for identification," E.O. 14086 and IC elements' implementing policies and procedures use both terms. Proclamation No. 14168, 90 Fed. Reg. 8615 (Jan. 20, 2025).

[33] E.O. 14086 § 2(b)(ii)(B).

[34] *Id*.

[35] According to ODNI, the ODNI CLPO's role in the review of the NIPF aligns with the ODNI CLPO's pre-existing responsibility to assess privacy and civil liberties safeguards concerning the activities of the IC and is similar to the ODNI CLPO's role under PPD- 28. Email from ODNI to PCLOB (May 1, 2025).

[36] E.O. 14086 § 2(b)(iii)(A).

[37] *Id*. § 2(b)(iii)(B).

been no instances in which the ODNI CLPO determined that a NIPF validated intelligence priority was likely not to meet the requirements of E.O. 14086 § 2(b)(iii).[38]

4. Privacy and Civil Liberties Safeguards

The Executive Order provides numerous privacy and civil liberties safeguards, including prioritizing targeted collection and placing limitations on bulk collection.[39] Specifically, it requires IC elements, in considering whether to collect signals intelligence, to "consider the availability, feasibility, and appropriateness of other less intrusive sources and methods for collecting the information necessary to advance a validated intelligence priority."[40] Signals intelligence collection activities "shall be as tailored as feasible to advance a validated intelligence priority and, taking due account of relevant factors, not disproportionately impact privacy and civil liberties."[41]

Further, bulk collection of signals intelligence shall be authorized only based on a determination "that the information necessary to advance a validated intelligence priority cannot reasonably be obtained by targeted collection."[42] If bulk collection is determined to be necessary, "reasonable methods and technical measures" must be applied "to limit the data collected to only what is necessary to advance a validated intelligence priority, while minimizing the collection of non-pertinent information."[43] For each IC element that collects signals intelligence in bulk, the Executive Order limits the use of such information to six legitimate objectives, which were carried forward from PPD-28.[44] The Executive Order

[38] Email from ODNI to PCLOB (May 14, 2025).

[39] *See supra* note 17 (defining bulk collection). Targeted collection activities are those directed against specific foreign intelligence targets through the use of discriminants, such as specific facilities, identifiers, or selection terms.

[40] E.O. 14086 § 2(c)(i)(A). Signals intelligence does not have to be the sole means available or used for advancing a validated intelligence priority.

[41] *Id*. § 2(c)(i)(B).

[42] *Id*. § 2(c)(ii)(A). The determination is made by "an element of the [IC] or through an interagency committee consisting in whole or in part of the heads of elements of the [IC], the heads of departments containing such elements, or their designees."

[43] *Id*.

[44] The six legitimate objectives for the use of signals intelligence collected in bulk under E.O. 14086 are:

> (1) [P]rotecting against terrorism, the taking of hostages, and the holding of individuals captive (including the identification, location, and rescue of hostages and captives) conducted by or on behalf of a foreign government, foreign organization, or foreign person; (2) protecting against espionage, sabotage, assassination, or other intelligence activities conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person; (3) protecting against threats from the development, possession, or proliferation of weapons of mass destruction or related technologies and threats conducted by, on behalf of, or with the assistance of a foreign government, foreign

addresses queries of bulk collection (but not queries of other types of collection), requiring that each element of the IC that conducts queries of unminimized signals intelligence obtained by bulk collection do so consistent with the six permissible uses of bulk collection.[45]

In addition, to enhance the legal, oversight, and compliance functions related to signals intelligence, E.O. 14086 mandates that each element of the IC that collects signals intelligence has senior-level legal, oversight, and compliance officials in place, including an inspector general and a privacy and civil liberties officer, who will conduct periodic oversight of signals intelligence activities, have the authority to conduct oversight of, and ensure compliance with, the law, and have access to all information pertinent to carrying out their oversight functions.[46] Each IC element must ensure that "significant incidents of non-compliance" are promptly reported to the element head, the agency head (to the extent relevant), and the DNI, who shall ensure that the incidents are remediated and recurrence prevented.[47] Additionally, each IC element must maintain appropriate training requirements to ensure that all personnel with access to signals intelligence know and understand the requirements of E.O. 14086 and the policies and procedures for reporting and remediating incidents of non-compliance.[48]

> organization, or foreign person; (4) protecting against cybersecurity threats created or exploited by, or malicious cyber activities conducted by or on behalf of, a foreign government, foreign organization, or foreign person; (5) protecting against threats to the personnel of the United States or of its allies or partners; and (6) protecting against transnational criminal threats, including illicit finance and sanctions evasion related to one or more of the other [bulk collection] objectives [. . .].

Id. § 2(c)(ii)(B).

[45] *Id*. § 2(c)(iii)(D). "Unminimized information" is defined as lawfully collected information for which a determination has not been made as to whether it contains foreign intelligence information or whether it may be otherwise retained pursuant to the IC element's minimization procedures. Off. of the Dir. of Nat'l Intel., *Annual Statistical Transparency Report Regarding Use of National Security Surveillance Authorities, Calendar Year 2024*, at 9 (2025), https://www.dni.gov/files/CLPT/documents/2025_ASTR_for_CY2024.pdf.

[46] E.O. 14086 § 2(d)(i)(A)-(B).

[47] *Id*. § 2(d)(iii)(A)-(B). In addition, to facilitate oversight and the redress process, each element of the IC that engages in signals intelligence collection activities must retain documentation, to the extent reasonable. Though the content of any such documentation may vary based on the circumstances, it shall, to the extent reasonable, provide the factual basis pursuant to which the IC element assessed that the collection was necessary to advance a validated intelligence priority. *Id*. § 2(c)(iii)(E).

[48] *Id*. § 2(d)(ii).

III. REVIEW OF POLICIES AND PROCEDURES

This report analyzes the IC elements' updated policies and procedures (implementing policies and procedures) to ensure that they are consistent with the Executive Order's enhanced safeguards. This review is based on information PCLOB gathered from IC elements in coordination with ODNI's CLPT. Eleven IC elements, including CIA, DEA ONSI, DHS I&A, DHS USCG, DOE-IN, FBI, NRO, NSA, ODNI, State INR, and Treasury OIA, updated their implementing policies and procedures in 2023.[49] The remaining seven IC elements, all of which are DoD components (i.e., DIA, NGA, and the intelligence elements of the five DoD services: the Army, Navy, Marine Corps, Air Force, and Space Force), were required by the Under Secretary of Defense for Intelligence and Security to conduct their signals intelligence activities governed by E.O. 14086 in accordance with NSA's implementing policies and procedures.[50]

In the course of our review, PCLOB examined significant additional relevant material, such as IC elements' supplemental guidance and trainings on E.O. 14086 implementation. PCLOB received additional materials and information from the following IC elements, agencies, and, departments during this review: CIA, DIA, DoD, DOE-IN, DHS I&A, DHS USCG, State INR, Treasury OIA, DEA ONSI, FBI, NRO, NSA, and ODNI. PCLOB also maintained continuous communication with IC elements and received oral clarification and written responses to its requests for information and questions.

This report focuses largely on the implementation of the policies and procedures updated pursuant to E.O. 14086 by NSA, CIA, and FBI.[51] While the Executive Order applies to every element of the IC, and PCLOB has assessed each element's implementing policies and procedures, the Executive Order has had the greatest impact on these three entities because they collect signals intelligence, or information that they consider to be covered by E.O. 14086, and possess or handle unevaluated signals intelligence.[52]

---

[49] *ODNI Releases Intelligence Community Procedures Implementing New Safeguards in Executive Order 14086*, *supra*.

[50] U.S. Dep't of Def., *Department of Defense Intelligence Community Element Compliance with Executive Order 14086, "Enhancing Safeguards for United States Signals Intelligence Activities"* (2023), https://www.intelligence.gov/assets/documents/702-documents/oversight/DoD_IC_Element_Compliance_with_E.O.14086.pdf.

[51] References to NSA in this report include NSA/Central Security Service (CSS) personnel and other members of the United States SIGINT System (USSS).

[52] While "unevaluated," or "raw," signals intelligence is not uniformly defined across the IC, DoD defines "unevaluated signals intelligence" as signals intelligence that has been collected but has not yet been evaluated to determine whether it can be retained. *See e.g.,* U.S. Dep't of Def., *DoD Manual S-5240.01-A, Procedures Governing the Conduct of DoD Intelligence Activities: Annex Governing Signals Intelligence*

This section assesses whether and how these updated E.O. 14086 policies and procedures, and their implementation, are consistent with the enhanced safeguards contained in the Executive Order. Its structure follows key phases of the intelligence data lifecycle: collection, use, retention, and dissemination. It also examines the application of IC elements' implementing policies and procedures, specifically as relates to documentation, training, oversight, and IC elements' ability to deviate and depart from these policies and procedures. This section does not exhaustively summarize the policies and procedures of each agency; rather it highlights key aspects of IC elements' policies and procedures and explains where differences emerge in the implementation of the Executive Order.

A. Collection

IC elements' implementing policies and procedures vary, but *all comport with or exceed* the signals intelligence collection safeguards set forth in E.O. 14086.

The IC elements' process for the collection of signals intelligence information has largely remained consistent with its process operated under PPD-28. The NIPF remains the primary mechanism to create, remove, communicate, and manage national intelligence priorities that guide IC collection and analytic activities.[53] PPD-28 Section 3 and its Classified Annex continue to supplement the signals intelligence priorities review and approval process. ODNI, through the semi-annual interagency review of intelligence priorities, establishes signals intelligence priorities and requirements. Policy makers consider the value of signals intelligence in light of risks entailed in conducting these activities, including those related to privacy and civil liberties.[54]

IC elements' implementing policies and procedures vary, but all comport with or exceed the signals intelligence collection safeguards set forth in E.O. 14086. The variations depend on whether and to what extent a particular IC element collects signals intelligence and the specific way in which an IC element uses that intelligence.

Information and Data Collected Pursuant to Section 1.7(c) of E.O. 12333, at 43 (2021), https://www.intelligence.gov/assets/documents/702-documents/declassified/Redacted%20Annex%20DODM%205240.01-A(1).pdf [hereinafter SIGINT Annex]; *see also infra* Section III(D) (Retention).

[53] Off. of the Dir. of Nat'l Intel., *Intel. Cmty. Directive 204, National Intelligence Priorities Framework*, at D.1 (Jan. 7, 2021), https://www.dni.gov/files/documents/ICD/ICD_204_National_Intelligence_Priorities_Framework_U_FINAL-SIGNED.pdf.

[54] *See e.g.*, Cent. Intel. Agency, *Collection, Use and Dissemination of Signals Intelligence*, at 5 (2024).

Three IC elements—NSA, CIA, and FBI—collect signals intelligence or information that is otherwise subject to E.O. 14086.[55]

1. NSA

NSA is the primary IC element responsible for the collection of signals intelligence. NSA's implementing policies and procedures limit signals intelligence collection to that which is necessary to obtain foreign intelligence to advance a validated intelligence priority and prioritize targeted over bulk collection. Specifically, NSA's implementing policies and procedures state that signals intelligence collection should, whenever practicable, be conducted using one or more selection terms to ensure that the collection efforts remain focused on specific foreign intelligence targets or topics (e.g., a specific, known international terrorist or terrorist group or the proliferation of weapons of mass destruction by a foreign power or its agents).[56]

Further, when NSA personnel determine that bulk collection is necessary to advance a validated intelligence priority, the bulk collection must nevertheless be as circumscribed as possible, proportionate to the intelligence objective, and as limited in duration as needed to satisfy the collection objective.[57] Specifically, bulk collection must be limited to circumstances where the NSA Director, or their designees, in consultation with the NSA CLPT Director, determines that "the information cannot reasonably be obtained by targeted collection or alternatives to SIGINT"; that "the information is necessary to advance a validated intelligence priority"; and that "reasonable methods and technical measures to limit the data collected to only what is necessary to advance a validated intelligence priority, while minimizing the collection of non-pertinent information, will be applied."[58]

Additionally, NSA's implementing policies and procedures apply not only to the collection of signals intelligence but also to the development of "SIGINT collection techniques"—a topic not explicitly addressed by E.O. 14086.[59] In so doing, NSA has expanded its application of E.O. 14086 protections to cover additional activities. Also, when conducting collection or developing collection techniques, NSA personnel are required "to consider . . . [w]hether

[55] Some IC elements apply E.O. 14086 more broadly than others. For example, as discussed below, FBI applies E.O. 14086 to its FISA Section 702 collection activities.

[56] Nat'l Sec. Agency, *NSA/CSS Policy 12-3 Annex C, Supplemental Procedures for the Collection, Processing, Querying, Retention, and Dissemination of Signals Intelligence Information and Data Containing Personal Information of Non-United States Persons*, at C-3 (2023) [hereinafter NSA/CSS Policy 12-3 Annex C].

[57] *Id*. at C-4.

[58] *Id*. at C-5.

[59] *Id*. at C-4.

additional approvals or civil liberties and privacy protections are needed" beyond those explicitly required under the Executive Order, as well as "the USSS entities responsible for implementing those requirements."[60]

2. CIA

CIA's supplemental guidance clarifies and elaborates upon the Executive Order's collection requirements in several respects. For example, the guidance elaborates upon the Executive Order's requirement that "targeted collection shall be prioritized" by directing that signals intelligence collection activities should be against specific foreign intelligence targets or topics through the use of discriminants, such as specific identifiers or selection terms.[61] Additionally, CIA's supplemental guidance clarifies certain collection-related processes. Authorizing bulk signals intelligence collection activities, for example, requires certification that the activities comply with E.O. 14086, PPD-28, NSM-15, and CIA's implementing policies and procedures and subsidiary guidance.[62]

Under CIA's supplemental guidance, at the collection planning phase of the intelligence data cycle, personnel are required to deconflict[63] planned signals intelligence collection activities against existing datasets across all collection disciplines, including diplomatic and public sources, amongst others, and consider whether the information is available from other sources. Per its policy, "CIA prioritize[s] appropriate and feasible alternatives to signals intelligence collection where practicable by means of the least intrusive technique required to obtain intelligence of the nature, reliability, and timeliness required."[64] CIA must also deconflict its proposed signals intelligence collection activities against PPD-28 restrictions and requirements.[65]

[60] *Id*.

[61] *Collection, Use and Dissemination of Signals Intelligence*, *supra*, at 4-5.

[62] *Id*. at 7.

[63] Deconfliction generally refers to the coordination of collection activities across the IC to ensure there is no collection overlap.

[64] *Collection, Use and Dissemination of Signals Intelligence*, *supra*, at 6. While NSA's implementing policies and procedures require NSA personnel to consider the availability, feasibility, and appropriateness of other less intrusive sources and methods for collecting the information necessary to advance a validated intelligence priority, including from diplomatic and public sources, NSA's implementing policies and procedures do not establish a deconfliction requirement similar to that of CIA. *NSA/CSS Policy 12-3 Annex C*, *supra*, at C-3.

[65] *Collection, Use and Dissemination of Signals Intelligence*, *supra*, at 6.

3. FBI

While FBI has a role in the IC's collection of Section 702 data, FBI does not otherwise collect signals intelligence.[66] Consistent with its application of PPD-28, FBI applies E.O. 14086 to its collection activities conducted under Section 702 of FISA.[67] Specifically, FBI must:

> [E]nsure that its activities under Section 702 are as tailored as feasible to advance a validated intelligence priority and, taking due account of relevant factors, do not disproportionately impact privacy and civil liberties. Such factors may include the nature of the pursued objective; the feasible steps taken to limit the scope of the collection to the authorized purpose; the intrusiveness of the collection activity, including its duration; the probable contribution of the collection to the objective pursued; the reasonably foreseeable consequences to individuals, including unintended third parties; the nature and sensitivity of the data to be collected; and the safeguards afforded to the information collected.[68]

As referenced above, FBI reported to PCLOB that because of the nature of the protections that are in place under FISA Section 702, including FBI's targeting, minimization, and querying procedures, FBI's acquisition of information subject to E.O. 14086 has been and remains in compliance with the Executive Order.[69]

NSA's role in FBI's Section 702 collection also helps to ensure that FBI's collection activities comply with the Executive Order, including its requirement that signals intelligence activities be conducted "only following a determination that a specific signals intelligence collection activity, based on a reasonable assessment of all relevant factors, is necessary to

[66] FBI has access to only a small fraction of the collection of Section 702-acquired information. As of September 2023, this was approximately 3.2 percent of the total number of Section 702 targets in 2022. 2023 PCLOB Section 702 Report, *supra*, at 77 (citing Off. of the Dir. of Nat'l Sec., *Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities, Calendar Year 2022*, at 22 (2023), https://www.dni.gov/files/CLPT/documents/2023_ASTR_for_CY2022.pdf ("FBI queries of Section 702 data do not run against the entirety of the IC's Section 702 collection. Rather, they only run against the subset of collection available to FBI—approximately 3.2% of Section 702 targets, as of February 2023.")). While FBI's limit on accessing the Section 702-acquired collection was previously only a policy, in 2024 Congress made this a statutory limitation. *See* Reforming Intelligence and Securing America Act, Pub. L. No. 118-49, §§ 2-3, 138 Stat. 862, 862-67 (2024). Congress's action followed the recommendation for codification by two PCLOB members. 2023 PCLOB Section 702 Report, *supra*, at B-49-B-57 (Recommendation 2).

[67] Fed. Bureau of Investigation, *Federal Bureau of Investigation Executive Order 14086 Implementing Policies and Procedures*, at 1 (2023) [hereinafter FBI Implementing Policies and Procedures].

[68] *Id.* at 2.

[69] PCLOB Phone Call with FBI (March 27, 2025).

advance a validated intelligence priority."[70] In order for FBI to target persons for collection under Section 702, NSA must determine, based on a particularized and fact-based assessment, that a significant purpose of the acquisition is to obtain foreign intelligence information.[71] Specifically, NSA must "reasonably assess, based on the totality of the circumstances, that the target is expected to possess, receive, and/or is likely to communicate foreign intelligence information concerning a foreign power or foreign territory authorized for targeting under a certification or authorization executed by the [DNI] and the Attorney General in the manner prescribed by section 702."[72]

PCLOB assesses that all IC elements that collect signals intelligence or information that is otherwise subject to E.O. 14086—NSA, CIA, and FBI—are compliant with the collection requirements of E.O. 14086. Though these IC elements' implementing policies and procedures vary based on the extent to which they collect signals intelligence, all comport with or exceed the signals intelligence collection safeguards set forth in E.O. 14086.

B. Documentation

E.O. 14086 requires that:

> [E]ach element of the [IC] that engages in signals intelligence collection activities shall maintain documentation to the extent reasonable in light of the nature and type of collection at issue and the context in which it is collected. The content of any such documentation may vary based on the circumstances but shall, to the extent reasonable, provide the factual basis pursuant to which the element of the [IC], based on a reasonable assessment of all relevant factors, assesses that the signals intelligence collection activity is necessary to advance a validated intelligence priority.[73]

This new documentation requirement is intended "to facilitate the oversight process . . . and the redress mechanism" established by E.O. 14086.[74]

---

[70] E.O. 14086 § 2(c)(i)(A).

[71] Fed. Bureau of Investigation, *Procedures Used by the Federal Bureau of Investigation for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended*, at 1 (July 2024).

[72] Nat'l Sec. Agency, *Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended*, at 5 (July 2024) [hereinafter 2024 NSA Targeting Procedures].

[73] E.O. 14086 § 2(c)(iii)(E).

[74] *Id*.

Each IC element that engages in signals intelligence collection (i.e., NSA, CIA, and FBI) has, through a combination of pre-existing policies and newly-issued E.O. 14086 policies and procedures, established documentation requirements that fulfill these criteria.

NSA incorporated the E.O. 14086 documentation requirement into its implementing policies and procedures nearly verbatim and with only two substantive changes, both of which serve to clarify the application of this requirement.

Each IC element that engages in signals intelligence collection has . . . *established documentation requirements* that are consistent with E.O. 14086.

First, NSA added language clarifying the Executive Order's statement that "[t]he content of any such documentation may vary based on the circumstances."[75] NSA's implementing policies and procedures note that "[f]or example, the content of documentation will likely differ depending upon the specific type of SIGINT collection activity, the location at which the activity is conducted, and the element of NSA/CSS or the USSS carrying out the SIGINT collection activity."[76]

Second, NSA's implementing policies and procedures explicitly reference a pre-existing documentation requirement to which NSA personnel must adhere with respect to signals intelligence collection conducted pursuant to E.O. 12333. The implementing policies and procedures state that, "consistent with existing requirements in . . . DoDM S-5240.01-A," which, with limited exception, applies to activities conducted under E.O. 12333, "NSA/CSS and USSS personnel will document and annually review the use of selection terms as the basis for collection to ensure compliance with applicable authorities, including Executive Order 14086."[77]

NSA's Section 702 targeting procedures also establish documentation requirements that are consistent with E.O. 14086. Under these targeting procedures, NSA analysts who request that persons be targeted for collection under Section 702 of FISA are required to:

> [P]rovide a written explanation of the basis for their assessment, at the time of targeting, that the target possesses, is expected to receive, and/or is likely to communicate foreign intelligence information concerning a foreign power or foreign territory authorized for targeting under a certification or

[75] *Id*.

[76] *NSA/CSS Policy 12-3 Annex C*, *supra*, at C-8.

[77] *Id*.

> authorization executed by the [DNI] and the Attorney General in the manner prescribed by section 702.[78]

CIA also incorporated the Executive Order's documentation requirement into its implementing policies and procedures nearly verbatim. However, unlike NSA, CIA supplemented its implementing policies and procedures with detailed supplemental guidance that serves both to limit, and in other ways expand, the scope of this requirement.

For example, CIA's supplemental guidance establishes additional requirements concerning the specific documentation that CIA personnel are required to complete pursuant to E.O. 14086 for certain signals intelligence collection activities.[79] However, these additional documentation requirements apply only to collection activities that CIA personnel are otherwise required to document under Section 5 of CIA's E.O. 12333 Attorney General-approved guidelines: namely, bulk signals intelligence collection[80] and "any other collection activity resulting in the acquisition of a quantity of information" that either "[e]xceeds the CIA's capability to evaluate the information promptly for retention" or "is determined to qualify for retention in its entirety without individualized review of the data contained within the set of collected information."[81] As a result, signals intelligence collection activities that are targeted and that result in a quantity of information that can be promptly reviewed, line-by-line, to determine whether the information qualifies for retention are not subject to the documentation requirements established by Section 5 of CIA's E.O. 12333 Attorney General-approved guidelines, nor are they subject to the equivalent E.O. 14086-related documentation requirements established by CIA's implementing policies and procedures.[82] PCLOB assesses that this limitation is reasonable, as it is consistent with E.O. 14086's requirement that IC elements maintain documentation not in all cases, but only "to the extent reasonable in light of the nature and type of collection at issue and the context in which it is collected."[83] Further, CIA informed PCLOB that the decision to utilize existing Attorney General Guidelines documentation process was intended, in part, to ensure that

[78] 2024 NSA Targeting Procedures, *supra*, at 5.

[79] *See* Cent. Intel. Agency, *Retention, Handling, and Training Requirements for Data Acquired Through Signals Intelligence*, at 6-7 (2024).

[80] *See* Cent. Intel. Agency, *Central Intelligence Agency Intelligence Activities: Procedures Approved by the Attorney General Pursuant to Executive Order 12333*, at 20-21 (2017). E.O. 12333 requires all IC elements to develop guidelines governing the collection, retention, and dissemination of information concerning U.S. persons that are approved by the Attorney General. Exec. Order No. 12,333 § 2.3.

[81] *Central Intelligence Agency Intelligence Activities: Procedures Approved by the Attorney General Pursuant to Executive Order 12333*, *supra*, at 20.

[82] Cent. Intel. Agency, E.O. 14086 Training.

[83] E.O. 14086 § 2(c)(iii)(E).

requirements applicable to U.S. persons aligned with those applicable to non-U.S. persons, which is consistent with the spirit of the Executive Order.[84]

Despite the limited scope of application of the Executive Order's documentation requirement to CIA signals intelligence collection activities, the information that CIA personnel are required to include in this documentation extends beyond what is explicitly required under E.O. 14086. CIA's supplemental guidance not only requires that personnel include, "[t]o the extent reasonable, the factual basis for assessing that the signals intelligence collection activity is necessary to advance a validated intelligence priority," as required by the Executive Order, but also requires the inclusion, "[t]o the extent reasonable" of "the factual basis for assessing that the signals intelligence collection activity . . . is as tailored as feasible" and "does not disproportionately impact privacy and civil liberties."[85] Additionally, if the documentation relates to a bulk signals collection activity, it must include:

> [A] statement that the information necessary to advance a validated intelligence priority cannot reasonably be obtained by targeted collection and that reasonable methods and technical measures will be applied to limit the data collected to only what is necessary to advance a validated intelligence priority, while minimizing the collection of non-pertinent information.[86]

Unlike NSA and CIA, FBI omitted much of the language in the Executive Order's documentation requirement from its E.O. 14086 implementing policies and procedures. The operative part of the requirement, as it appears in FBI's implementing policies and procedures, states simply that "the FBI shall maintain appropriate documentation with respect to its activities under Section 702 of FISA, including the documentation required by the FBI's Section 702 Standard Minimization Procedures, the FBI's Section 702 Targeting Procedures, and the FBI's Section 702 Querying Procedures."[87] However, as discussed above, NSA—not FBI—makes the necessary determination regarding the foreign intelligence purpose of FBI acquisitions under Section 702. And, as also discussed above, NSA has policies and procedures in place to ensure these determinations are documented consistent with the requirements of E.O. 14086. For this reason and because the only information subject to E.O. 14086 that FBI collects is Section 702 data,[88] PCLOB assesses that the lack of more detailed documentation language in FBI's implementing policies and procedures is reasonable.

---

[84] PCLOB Phone Call with CIA (May 21, 2025).

[85] *Retention, Handling, and Training Requirements for Data Acquired Through Signals Intelligence*, *supra*, at 6-7.

[86] *Id.* at 7.

[87] FBI Implementing Policies and Procedures, *supra*, at 4.

[88] As mentioned above, FBI has access to only a small fraction of the collection of Section 702-acquired information—as of September 2023, approximately 3.2 percent. 2023 PCLOB Section 702 Report, *supra*, at 77

PCLOB assesses that each IC element that engages in signals intelligence collection has established documentation requirements that are consistent with E.O. 14086.

C. Use

E.O. 14086 requires that each IC element handling personal information collected through signals intelligence abide by various data security and access requirements. In particular, IC elements must provide protection for the data and prevent unauthorized access, limit access to those who have a need-to-know, and ensure that personal information for which no final retention determination has been made is accessed only for the purpose of making a retention determination (or other authorized administrative purposes).[89] Other use requirements and limitations in the E.O. include maintaining data quality[90] and limiting queries of bulk collection to the permissible objectives for bulk collection.[91]

All IC elements' implementing policies and procedures meet these use requirements as laid out in E.O. 14086. The IC elements that regularly handle signals intelligence adhered most closely to the Executive Order's requirements by adapting the language almost verbatim[92] in their implementing policies and procedures, to include CIA, FBI, NSA, and ODNI.[93]

The remaining IC elements included the requirements with some minor exceptions and variations. Because they are non-collectors of signals intelligence information and therefore only receive final intelligence products, DEA, DOE, DHS I&A, INR, NRO, Treasury OIA, and USCG all omitted the requirement that personal information collected through signals intelligence for which no final retention determination has been made is accessed only in order to make such a determination.[94] (Decisions surrounding retention are made by

(citing *Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities, Calendar Year 2022*, *supra*, at 22 ("FBI queries of Section 702 data do not run against the entirety of the IC's Section 702 collection. Rather, they only run against the subset of collection available to the FBI—approximately 3.2% of Section 702 targets, as of February 2023.")).

[89] E.O. 14086 § 2(c)(iii).

[90] *Id.* § 2(c)(iii)(C).

[91] *Id.* § 2(c)(iii)(D).

[92] Language changes were merely to adapt the requirements to their policies and were non-substantive in these cases.

[93] *Retention, Handling, and Training Requirements for Data Acquired Through Signals Intelligence, supra,* at 9; FBI Implementing Policies and Procedures, *supra,* at 7; *NSA/CSS Policy 12-3 Annex C*, *supra*, at C-6; Off. of the Dir. of Nat'l Intel., *Office of the Director of National Intelligence Executive Order 14086 Policies and Procedures*, at 4 (2023), https://www.intelligence.gov/assets/documents/702-documents/oversight/ODNI_EO14086_PP.pdf [hereinafter ODNI Implementing Policies and Procedures].

[94] Drug Enforcement Admin. Off. of Nat'l Sec. Intel., *Executive Order 14086—Policy and Procedure*, at 4-5 (2023), https://www.intelligence.gov/assets/documents/702-

collectors before dissemination of the relevant intelligence products.) Notably, NRO's implementing policies and procedures include the qualification that access to personal information collected through signals intelligence activities "when identifiable" is restricted to those who need to know such disseminated signals intelligence information in the performance of authorized duties in support of NRO's mission, highlighting the fact that NRO does not collect and query signals intelligence information that will result in access to personal information.[95]

All IC elements' implementing policies and procedures meet the Executive Order's requirements with regard to queries. Because E.O. 14086 does not discuss queries[96] other than those conducted to review unminimized bulk collection,[97] most IC elements did not address queries conducted on targeted collection in their implementing policies and procedures. NSA went beyond the E.O.'s requirements, however, by providing guidelines for all queries, listing various categories and the relevant authorities and requirements for

documents/oversight/DEA_ONSI_EO_14086.pdf [hereinafter DEA Implementing Policies and Procedures]; U.S. Dep't of Energy Off. of Intel. and Counterintelligence, *Policy and Procedures Implementing Executive Order 14086 Regarding Use, Maintenance and Handling of signals Intelligence* Information, at 3-4 (2023), https://www.intelligence.gov/assets/documents/702-documents/oversight/Energy_INPG_EO_14086_Policy.pdf [hereinafter DOE-IN Implementing Policies and Procedures]; U.S. Dep't of Homeland Sec. Off. of Intel. and Analysis, *Safeguarding Personal Information Collected from Signals Intelligence Activities*, at 4-5 (2023), https://www.intelligence.gov/assets/documents/702-documents/oversight/DHS_IA_EO_14086_PP.pdf [hereinafter DHS I&A Implementing Policies and Procedures]; U.S. Dep't of State Bureau of Intel. and Res., *Executive Order 14086 – Policy and Procedures*, at 4-5 (2023), https://www.intelligence.gov/assets/documents/702-documents/oversight/State_INR_EO_14086_PP.pdf [hereinafter State INR Implementing Policies and Procedures]; Nat'l Reconnaissance Off., *Executive Order 14086 – Enhancing Safeguards for United States Signals Intelligence Activities*, at 3-4 (2023), https://www.intelligence.gov/assets/documents/702-documents/oversight/NRO_EO_14086_PP.pdf [hereinafter NRO Implementing Policies and Procedures]; U.S. Dep't of Treasury Off. of Intel. and Analysis, *Safeguarding Personal Information Collected Through Signals Intelligence*, at 3-4 (2023), https://www.intelligence.gov/assets/documents/702-documents/oversight/Treasury_OIA_EO_14086_Policy.pdf [hereinafter Treasury OIA Implementing Policies and Procedures]; U.S. Coast Guard, *Procedures Implementing Enhanced Safeguards for Signals Intelligence Activities Under Executive Order 14086*, at 4-5 (2023), https://www.intelligence.gov/assets/documents/702-documents/oversight/USCG_EO_14086_Signed.pdf [hereinafter DHS USCG Implementing Policies and Procedures].

[95] NRO Implementing Policies and Procedures, *supra*, at 4.

[96] Queries allow trained IC personnel to identify specific information in the collected data and view specific results and are therefore one of the primary ways they analyze signals intelligence information. Off. of the Dir. of Nat'l Intel., *FISA Section 702: Finding the Foreign Intelligence Information,* https://www.intel.gov/assets/documents/fisa/Finding_Foreign_Intelligence_Information_Section_702_FISA_Resource_Library.pdf (last visited Sept. 22, 2025).

[97] E.O. 14086 § 2(c)(iii)(D).

each.[98] For all queries using selection terms that identify any person regardless of nationality and residence, NSA has added a provision that queries "shall be designed to defeat, to the extent practicable under the circumstances, the retrieval of personal information that is not relevant, necessary, nor proportionate to advance a validated intelligence priority," as listed in the Executive Order.[99]

D. Retention

All IC elements have complied with the requirements of E.O. 14086 by *aligning retention of non-U.S. person data* to the same standards and timeframes as that of U.S. person data.

E.O. 14086 requires that each IC element handling personal information collected through signals intelligence abide by three general retention rules: (1) retain non-U.S. person data only if retention of comparable U.S. person data would be permitted, and under the same retention periods for U.S. persons; (2) non-U.S. person personal data for which no final retention determination has been made is subject to the same temporary retention periods as that of U.S. persons; and (3) the element must delete non-U.S. person personal data if comparable U.S. person data must be deleted.[100] In other words, as indicated above, E.O. 14086 brings retention of non-U.S. person data up to the standards required for U.S. persons.

These three retention requirements are similar to what was in place under PPD-28. However, rather than a requirement of deletion (E.O. 14086's third requirement), PPD-28 merely required that unevaluated information be retained for no longer than five years unless the DNI expressly determined that continued retention was in the interest of national security.[101] After the issuance of PPD-28, the Intelligence Authorization Act of 2015 also specified a detailed retention framework for retaining "covered communications"[102] of U.S. persons, with the default for unevaluated signals intelligence being a five-year retention period.[103]

---

[98] NSA/CSS Policy 12-3 Annex C, *supra*, at C-6.

[99] *Id*.

[100] E.O. 14086 § 2(c)(iii)(A)(2).

[101] PPD-28, *supra*, at § 4(a)(i).

[102] A "covered communication" is defined in the IAA as "nonpublic telephone or electronic communication acquired without the consent of a person who is a party to the communication, including communications in electronic storage." 50 U.S.C. § 1813.

[103] *Id*. Additionally, following PPD-28, ODNI issued Intelligence Community Standard (ICS) 107-01, a policy governing requests for extensions beyond the five-year retention period, which required DNI approval for

Each IC element sets its own retention schedules, which are specified in the IC elements' respective FISA minimization procedures and E.O. 12333 Attorney General-approved guidelines. Retention schedules vary for different types of data (e.g., evaluated vs. unevaluated, Section 702 data vs. other signals intelligence). All IC elements' implementing policies and procedures comply with the Executive Order's retention requirements, though some policies take slightly different approaches, and each applies its own underlying retention schedule to U.S. person data.

Each IC element incorporated the E.O. 14086 retention requirements in a dedicated section of its relevant policy document, with some slight variations. CIA's and FBI's[104] implementing policies and procedures contain the retention requirements from E.O. 14086[105] listed above nearly verbatim, with very minor non-substantive changes to adapt the Executive Order's requirements to their respective policies.[106]

NSA's implementing policies and procedures summarize the retention requirements from the "SIGINT Annex" for E.O. 12333, which are the same as the requirements under E.O. 14086.[107] The SIGINT Annex provides a detailed retention schedule for U.S. person

extensions to retain unevaluated signals intelligence data for 20 years. *See* Off. of the Dir. of Nat'l Sec., *Intelligence Community Standard 107-01: Continued Retention of SIGINT Under PPD-28* (2015), https://www.dni.gov/files/documents/ppd-28/ICS%20107-1.pdf. After Congress enacted changes to 50 U.S.C. § 1813 in 2015, retention of U.S. person data beyond the five-year period requires approval by the relevant IC agency head. ICS 107-01 was rescinded after the issuance of E.O. 14086 to make the requirements for U.S. persons and non-U.S. persons consistent.

[104] Because the only raw intelligence information subject to E.O. 14086 that FBI handles is Section 702 data, FBI's retention practices for such information are governed by its Section 702 minimization procedures and supplemented by E.O. 14086. According to FBI's Section 702 minimization procedures, its retention schedule is: in general, after five years all FISA information that has not been reviewed will be destroyed, after 10 years access to information that has been reviewed but not identified as meeting the applicable standard will be limited and require additional approvals to be fully accessible for authorized personnel, and after 15 years information that has been retained and reviewed but not yet identified as information that reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or its importance, or to be evidence of a crime, will be destroyed. Fed. Bureau of Investigation, *Minimization Procedures Used by the FBI in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended*, at 18 (2024).

[105] E.O. 14086 § 2(c)(iii)(A)(2).

[106] A handful of agencies also included a definition of retention in their policy: ODNI, NRO, DOE-IN, and USCG. Each of these agencies defined "retention" in the same words: "retention shall mean the maintenance of signals intelligence in either hard copy or electronic format regardless of how the information was collected." ODNI Implementing Policies and Procedures, *supra*, at 3.

[107] *NSA/CSS Policy 12-3 Annex C*, *supra*, at C-7.

information and implements Section 309 of the Intelligence Authorization Act 2015, which laid out this retention schedule in statute.[108]

A number of agencies included the three retention requirements of E.O. 14086, while adding into their retention policies requirements from elsewhere in the Executive Order that personal information both must relate to an authorized intelligence requirement and cannot be retained solely because of the non-U.S. person's foreign status. NSA, ODNI, DEA, NRO, DOE-IN, DHS I&A, USCG, State INR, and Treasury OIA all added such a provision.[109]

PCLOB assesses that all IC elements have complied with the requirements of E.O. 14086 by aligning retention of non-U.S. person data to the same standards and timeframes as that of U.S. person data.

E. Dissemination

E.O. 14086 requires that the dissemination of personal information collected through signals intelligence shall be minimized by limiting both the extent of dissemination and the types of information that may be disseminated. Specifically, it states that "[e]ach element of the [IC] that handles personal information collected through signals intelligence shall establish and apply policies and procedures designed to minimize the dissemination . . . of personal information collected through signals intelligence."[110] The Executive Order also provides that IC elements that handle personal information collected through signals intelligence:

> [S]hall disseminate non-United States persons' personal information collected through signals intelligence only if it involves one or more of the comparable types of information that section 2.3 of Executive Order 12333 of December 4, 1981 (United States Intelligence Activities), as amended, states may be disseminated in the case of information concerning United States persons.[111]

---

[108] 50 U.S.C. § 1813(a)(1).

[109] *NSA/CSS Policy 12-3 Annex C, supra,* at C-7; ODNI Implementing Policies and Procedures, *supra*, at 3-4; DEA Implementing Policies and Procedures, *supra*, at 4; DOE-IN Implementing Policies and Procedures, *supra*, at 3; DHS I&A Implementing Policies and Procedures, *supra*, at 5; State INR Implementing Policies and Procedures, *supra*, at 4; NRO Implementing Policies and Procedures, *supra*, at 4; Treasury OIA Implementing Policies and Procedures, *supra*, at 3; DHS USCG Implementing Policies and Procedures, *supra*, at 5.

[110] E.O. 14086 § 2(c)(iii)(A).

[111] *Id*. § 2(c)(iii)(A)(1)(a). Section 2.3 of E.O. 12333 states that the following types of information concerning U.S. persons may be disseminated:

> (a) Information that is publicly available or collected with the consent of the person concerned;
>
> (b) Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations . . .

These requirements build on the framework in place under PPD-28.[112] E.O. 14086 goes a step further, however, by including four provisions that further restrict the dissemination of personal information collected through signals intelligence. Specifically, under E.O. 14086, IC elements that handle personal information collected through signals intelligence: (1) may not disseminate this information "solely because of a person's nationality or country of residence";[113] (2) may not disseminate this information "for the purpose of circumventing" the Executive Order;[114] (3) may disseminate this information within the U.S. government "only if an authorized and appropriately trained individual has a reasonable belief that the personal information will be appropriately protected and that the recipient has a need to know the information";[115] and (4) must "take due account of the purpose of the dissemination, the nature and extent of the personal information being disseminated, and the potential for harmful impact on the person or persons concerned" before disseminating

> (c) Information obtained in the course of a lawful foreign intelligence, counterintelligence, international drug or international terrorism investigation;
>
> (d) Information needed to protect the safety of any persons or organizations, including those who are targets, victims, or hostages of international terrorist organizations;
>
> (e) Information needed to protect foreign intelligence or counterintelligence sources, methods, and activities from unauthorized disclosure . . .
>
> (f) Information concerning persons who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility;
>
> (g) Information arising out of a lawful personnel, physical or communications security investigation;
>
> (h) Information acquired by overhead reconnaissance not directed at specific United States persons;
>
> (i) Incidentally obtained information that may indicate involvement in activities that may violate federal, state, local, or foreign laws; and
>
> (j) Information necessary for administrative purposes.

Exec. Order No. 12,333 § 2.3.

[112] PPD-28 required that "IC elements . . . establish policies and procedures reasonably designed to minimize the dissemination and retention of personal information collected from signals intelligence activities." The Directive also stipulated that "[p]ersonal information shall be disseminated only if the dissemination of comparable information concerning U.S. persons would be permitted under section 2.3 of Executive Order 12333." PPD-28, *supra*, at § 4(a)(i).

[113] E.O. 14086 § 2(c)(iii)(A)(1)(b).

[114] *Id*. § 2(c)(iii)(A)(1)(e).

[115] *Id*. § 2(c)(iii)(A)(1)(c).

this information "to recipients outside the United States Government, including to a foreign government or international organization."[116]

Notwithstanding these restrictions, Section 5(d) of E.O. 14086 provides for an important exception, stating:

> Nothing in this order prohibits elements of the [IC] from disseminating information relating to a crime for law enforcement purposes; disseminating warnings of threats of killing, serious bodily injury, or kidnapping; disseminating cyber threat, incident, or intrusion response information; notifying victims or warning potential victims of crime; or complying with dissemination obligations required by statute, treaty, or court order, including orders of and procedures approved by the [U.S. Foreign Intelligence Surveillance Court (FISC)] or other court orders.[117]

As discussed below, every IC element included in PCLOB's review has either established or, pursuant to PPD-28 or other authorities, already had in place dissemination restrictions that fulfill, and in some cases exceed, the requirements of E.O. 14086. While there are many examples of IC elements omitting certain dissemination-related E.O. 14086 language from their implementing policies and procedures, PCLOB considers these omissions to be reasonable, because the omitted language relates to dissemination authorities or limitations that were already being applied pursuant to pre-existing legal authorities.

Additionally, IC elements have taken a variety of steps to assist personnel with the interpretation and application of E.O. 14086 dissemination requirements. The Executive Order's requirements are reflected in the updated policies and procedures that IC elements adopted pursuant to E.O. 14086, in their E.O. 14086-related trainings, and in the supplemental guidance that some IC elements have issued. While there is considerable overlap in the approach IC elements took to operationalize the Executive Order's dissemination requirements, there are notable differences in their implementation efforts.

Every IC element included in PCLOB's review has . . . in place *dissemination restrictions* that fulfill, and in some cases exceed, the requirements of E.O. 14086.

First, most IC elements have updated their policies and procedures or supplemental guidance in ways that do more to limit the dissemination of personal information collected

[116] *Id.* § 2(c)(iii)(A)(1)(d).

[117] *Id.* § 5(d).

through signals intelligence than is strictly required under E.O. 14086. This is an encouraging development, and one that is consistent with E.O. 14086's authorization for "the application of more privacy-protective safeguards" than those required under the Executive Order.[118]

CIA, for example, chose to apply not only the Executive Order's dissemination requirements but also its restrictions on the use of bulk signals intelligence to the dissemination of certain information. CIA's supplemental guidance on E.O. 14086 implementation states that the first dissemination of evaluated information collected from signals intelligence obtained by bulk collection constitutes a "use" of bulk signals intelligence.[119] As a result, when CIA disseminates evaluated information collected from signals intelligence obtained by bulk collection for the first time, it must not only adhere to E.O. 14086's dissemination requirements but must also satisfy at least one of the legitimate objectives of bulk signals intelligence.[120]

Additionally, seven IC elements—DEA ONSI, DHS I&A, DOE-IN, ODNI, State INR, Treasury OIA, and USCG—included additional dissemination restrictions relating to authorized intelligence requirements in their implementing policies and procedures that are not explicitly prohibited in E.O. 14086. Each of these elements' implementing policies and procedures states that if the element is disseminating personal information of a non-U.S. persons on the basis that it is foreign intelligence, the information must relate to an "authorized intelligence requirement."[121]

A second notable aspect of E.O. 14086 implementation as it relates to dissemination is that most IC elements omitted at least some of the Executive Order's dissemination language from their implementing policies and procedures. While these omissions might facially be regarded as potential implementation gaps, PCLOB does not consider this to be the case, as existing legal authorities already established limitations on dissemination.

Nearly all IC elements omitted language from Section 5(d) of E.O. 14086 from their implementing policies and procedures. As discussed above, Section 5(d) states that nothing in E.O. 14086 prohibits IC elements from disseminating information in certain circumstances, such as when an IC element is disseminating crime-related information for

---

[118] *Id*. § 5(c).

[119] Cent. Intel. Agency, *Collection, Use, and Dissemination of Signals Intelligence*, at 8 (2024).

[120] *Id*. at 8.

[121] DEA Implementing Policies and Procedures, *supra*, at 3; DHS I&A Implementing Policies and Procedures, *supra*, at 4; DOE-IN Implementing Policies and Procedures, *supra*, at 3; ODNI Implementing Policies and Procedures, *supra*, at 3; State INR Implementing Policies and Procedures, *supra*, at 3; Treasury OIA Implementing Policies and Procedures, *supra*, at 3; DHS I&A Implementing Policies and Procedures, *supra*, at 4; DHS USCG Implementing Policies and Procedures, *supra*, at 4.

law enforcement purposes or complying with dissemination obligations required by statute or court order.[122] Only one IC element—FBI—included the language from Section 5(d) in its entirety in its implementing policies and procedures.[123]

Relatedly, NSA omitted certain language from its implementing policies and procedures concerning disseminations within the U.S. government. E.O. 14086 states that IC elements "shall disseminate within the United States Government personal information collected through signals intelligence only if an authorized and *appropriately trained* individual has a reasonable belief that the personal information will be appropriately protected and that the recipient has a need to know the information" (emphasis added).[124] However, NSA did not include this "appropriately trained" language in the relevant section of its implementing policies and procedures.

PCLOB does not consider these omissions to represent deficiencies in IC elements' implementation of E.O. 14086. In response to questions posed by PCLOB in briefings with IC elements, IC officials indicated that the omitted language concerned authorities or limitations that were already being applied to the dissemination of personal information collected through signals intelligence pursuant to pre-existing legal authorities. The types of disseminations that Section 5(d) indicates are not prohibited by E.O. 14086, for instance, were already, and continue to be, governed by statutory authorities, such as FISA, which cannot be superseded by Executive Order; E.O. 12333, which remains in force; and IC elements' existing FISA minimization procedures. Likewise, while NSA's implementing policies and procedures do not explicitly incorporate E.O. 14086's "appropriately trained" language, these policies and procedures do state that "non-U.S. persons' personal information collected through SIGINT, may only be disseminated . . . consistent with existing

[122] E.O. 14086 § 5(d).

[123] FBI Implementing Policies and Procedures, *supra*, at 3 n. 2. An additional three IC elements—CIA, DEA ONSI, and ODNI—incorporated at least some elements of Section 5(d) in either their implementing policies and procedures, supplemental guidance, or trainings. CIA alluded to Section 5(d)'s allowance for statutorily required disseminations in its supplemental guidance, which states that CIA may disseminate non-U.S. persons' personal information collected through signals intelligence if the dissemination of comparable U.S. persons information would be permitted under FISA. *Collection, Use, and Dissemination of Signals Intelligence*, *supra*, at § 1(C)(1)(b)(1). DEA ONSI alluded to Section 5(d)'s allowance for the dissemination of crime-related information for law enforcement purposes in its implementing policies and procedures, which states that "[n]othing in these procedures shall prohibit or regulate DEA's activities pursuant to its statutory criminal law enforcement and civil regulatory missions," including "DEA's responsibilities pertaining to law enforcement information related to the domestic or foreign activities of U.S. persons." DEA Implementing Policies and Procedures, *supra*, at 3. Similarly, the E.O. 14086-related training administered by ODNI states that information concerning non-U.S. persons that reasonably appears to be evidence of a crime may be disseminated for law enforcement purposes. Off. of the Dir. of Nat'l Sec., *Basic and Raw FISA Training*, at 13 (2024).

[124] E.O. 14086 § 2(c)(iii)(A)(1)(c).

requirements in . . . DoDM S-5240.01-A . . . and other applicable [IC] and USSS dissemination standards and directives."[125] These "existing requirements" include a requirement that personal information only be disseminated by personnel who have received training on dissemination procedures.[126]

Moreover, there may be benefits to incorporating these pre-existing authorities and restrictions by reference. NSA officials, for instance, informed PCLOB that they intentionally sought to limit the "re-mirroring" of pre-existing policy language during the development of NSA's implementing policies and procedures, as they did not want to have their analysts be "too far away from" the original language, and wanted to instead encourage them to refer to source documents for authoritative guidance.[127]

A third notable aspect of the approach IC elements took to implement the Executive Order's dissemination requirements is that every IC element included in PCLOB's review has provided its personnel with element-specific information and guidance on the interpretation and practical application of the order's dissemination requirements.

For example, all IC elements provided a definition of "dissemination" in their implementing policies and procedures or supplemental guidance,[128] or (in the case of DHS I&A and NSA) clearly indicated where such a definition can be found in existing policy guidance.[129]

Additionally, two IC elements—State INR and Treasury OIA—have provided personnel with additional guidance for implementing the Executive Order's requirements for disseminating personal information collected through signals intelligence within the U.S. government. As discussed above, E.O. 14086 permits such dissemination "only if an authorized and appropriately trained individual has a reasonable belief that the personal information will be appropriately protected and that the recipient has a need to know the information."[130] While E.O. 14086 does not specify what constitutes an "appropriately trained individual,"

---

[125] *NSA/CSS Policy 12-3 Annex C*, *supra*, at C-7.

[126] U.S. Dep't of Def., *DoDM 5240.01, DoD Intelligence Activities*, at 20 (2019).

[127] PCLOB Phone Call with NSA (Apr. 11, 2025).

[128] Fed. Bureau of Investigation, *Foreign Intelligence Surveillance Act and Standard Minimization Procedures Policy Guide*, at § 5.17.2 (2024); Cent. Intel. Agency, *Collection, Use and Dissemination of Signals Intelligence*, *supra*, at 2; DEA Implementing Policies and Procedures, *supra*, at 4; NRO Implementing Policies and Procedures, *supra*, at 3; ODNI Implementing Policies and Procedures, *supra*, at 3; DOE-IN Implementing Policies and Procedures, *supra*, at 3; DHS I&A Implementing Policies and Procedures, *supra*, at 3; State INR Implementing Policies and Procedures, *supra*, at 4; Treasury OIA Implementing Policies and Procedures, *supra*, at 8.

[129] DHS I&A Implementing Policies and Procedures, *supra*, at 2; NSA/CSS Policy 12-3 Annex C, *supra*, at C-14.

[130] E.O. 14086 § 2(c)(iii)(A)(1)(c).

both State INR and Treasury OIA note in their E.O. 14086 trainings that, for purposes of applying this provision of the Executive Order, the disseminator must specifically be up to date on required annual E.O. 12333, Sensitive Compartmented Information, and E.O. 14086 trainings.[131]

Relatedly, one IC element—CIA—has developed additional guidance for implementing the Executive Order's requirements for disseminating personal information collected through signals intelligence outside of the U.S. government, including to foreign governments or international organizations, in cases where national security considerations may conflict with limitations on dissemination.[132] Specifically, "[f]or information being disseminated to a foreign or international organization," CIA personnel are required to "[c]onsider the importance of the disclosure to the national security of the US" and to "[m]ake a determination . . . which recognizes that the national security of the US may require dissemination of personal information collected through signals intelligence to foreign entities whose safeguards do not meet our standards."[133]

Based on its review, PCLOB assesses that each IC element that handles personal information collected through signals intelligence has in place dissemination policies and procedures that fulfill the requirements of E.O. 14086.

F. Training

E.O. 14086 requires that "[e]ach element of the [IC] shall maintain appropriate training requirements to ensure that all employees with access to signals intelligence know and understand the requirements of this order and the policies and procedures for reporting and remediating incidents of non-compliance with applicable United States law."[134] Additionally, each IC element that handles personal information collected through signals intelligence shall *inter alia* "limit access to such personal information to authorized personnel who . . . have received appropriate training on the requirements of applicable United States law."[135]

All IC elements have required training under PPD-28 since its issuance and have continued to maintain and require this PPD-28 training while updates were made to reflect new policy, process, and responsibility requirements under E.O. 14086. As of the date of this report, all

[131] U.S. Dep't of the Treasury Off. of Intel. and Analysis, *E.O. 14086 Annual Training*, at 7; U.S. Dep't of State, *INR Training for E.O. 14086* (2024).

[132] E.O. 14086 § 2(c)(iii)(A)(1)(d).

[133] *Collection, Use, and Dissemination of Signals Intelligence, supra*, at 10-11.

[134] E.O. 14086 § 2(d)(ii).

[135] *Id*. § 2(c)(iii)(B)(2).

IC elements have either deployed an E.O. 14086-specific training or have incorporated E.O. 14086 training into existing training materials. In their respective trainings, IC elements outline the requirements of E.O. 14086 as they relate to the role of the particular IC element in the intelligence lifecycle, pursuant to their E.O. 12333 authorities; address how IC elements' implementing policies and procedures, and supplemental guidance as applicable, protect the privacy rights of U.S. persons and non-U.S. persons under E.O. 14086; and provide insight as to the requirements for retention, necessity and proportionality, and bulk collection. Depending on the IC element, such training is conducted in-person or via a web-based platform.

However, IC elements differ as to how often applicable personnel[136] must complete training on E.O. 14086. CIA requires that training be completed every two years;[137] ODNI, NSA, DEA ONSI, DHS I&A, DIA, DoE, NRO, State INR, USCG, and Treasury OIA require that training be completed annually;[138] and while FBI personnel must complete annual training on the use of Section 702-derived collections, FBI personnel are not subject to continued training requirements specific to E.O. 14086 after the initial training required for personnel to gain access to signals intelligence data.[139]

Significant *variations in training requirements or lack of refresher training* could contribute to problematic gaps in implementation.

In addition, after updating intelligence oversight training to include E.O. 14086 requirements, some IC elements have required personnel to retake the updated training within a certain time period. For example, upon updating its training to include E.O. 14086, NRO initiated an agency-wide requirement to retake the mandatory intelligence oversight training with the newly included E.O. 14086-specific requirements within 45 days.[140] Similarly, following the launch of CIA's updated E.O. 14086 training, CIA officers with access

[136] Some IC elements require that training be completed by all IC element personnel who have access to information collected through signals intelligence activities, while others require that all IC element personnel complete this training regardless of whether they have access to signals intelligence.

[137] IC Written Responses to PCLOB Questions, at 3 (Dec. 4, 2024).

[138] IC Written Responses to PCLOB Questions, at 2 (Feb. 28, 2025); IC Written Responses to PCLOB Questions, at 2 (Feb. 21, 2025); IC Written Responses to PCLOB Questions, at 2 (Jan. 31, 2025); IC Written Responses to PCLOB Questions, at 2 (Dec. 4, 2024); IC Written Responses to PCLOB Questions, at 2 (Nov. 18, 2024).

[139] PCLOB Phone Call with FBI (March 27, 2025); *see Foreign Intelligence Surveillance Act and Standard Minimization Procedures Policy Guide, supra*, at 135.

[140] IC Written Responses to PCLOB Questions, Attachment D (Dec. 4, 2024).

to signals intelligence data and tools who had not taken the updated training were given a month to take the new course or lose their access.[141]

Access to information collected through signals intelligence activities is restricted to those personnel who have completed their respective IC element's mandatory training, which includes training on the requirements of E.O. 14086. All IC elements monitor the completion of training requirements to ensure compliance with E.O. 14086 and their implementing policies and procedures. In cases where an individual fails to complete the mandatory training, the individual may be subject to administrative action, such as loss of access to the system access and/or to signals intelligence data, and their supervisor may be notified of this noncompliance.

Although the ways in which IC elements implement E.O. 14086 will understandably vary given their various missions and authorities, PCLOB assesses that all IC elements have implemented the requisite training to ensure that all personnel with access to signals intelligence know and understand the Executive Order's requirements and the policies and procedures for reporting and remediating incidents of non-compliance. Though the Executive Order does not dictate the periodicity of trainings, significant variations in training requirements or lack of refresher training could contribute to problematic gaps in implementation.

G. Oversight

E.O. 14086 lists several requirements for IC elements relating to oversight and compliance "to build on the oversight mechanisms that IC elements already have in place and to further ensure that signals intelligence activities are subjected to rigorous oversight."[142] As referenced above, E.O. 14086 requires that each IC element that collects signals intelligence:

> (A) [S]hall have in place senior-level legal, oversight, and compliance officials who conduct periodic oversight of signals intelligence activities, including an Inspector General, a Privacy and Civil Liberties Officer, and an officer or officers in a designated compliance role with the authority to conduct oversight of and ensure compliance with applicable United States law;
>
> (B) shall provide such legal, oversight, and compliance officials access to all information pertinent to carrying out their oversight responsibilities, consistent with the protection of intelligence sources or methods, including their oversight responsibilities to ensure that any appropriate actions are

[141] CIA Response to PCLOB Questions (May 9, 2025).

[142] E.O. 14086 § 2(d).

taken to remediate an incident of non-compliance with applicable United States law; and

(C) shall not take any actions designed to impede or improperly influence such legal, oversight, and compliance officials in carrying out their oversight responsibilities.[143]

All IC elements that collect signals intelligence—NSA, FBI, and CIA—have in place multiple senior-level legal, oversight, cybersecurity, and compliance officials who conduct periodic oversight of signals intelligence activities and ensure compliance with applicable U.S. law.

All IC elements have implemented sufficient internal processes to ensure *compliance, review, and oversight* of signals intelligence activities conducted by IC element personnel.

NSA's signals intelligence activities are overseen by NSA's Inspector General, General Counsel, Civil Liberties, Privacy, and Transparency Officer, and Directors of Operations and Cybersecurity, who review signals intelligence production activities and practices, periodically audit such activities and practices against the standards required by E.O. 14086, and participate in the development of appropriate documentation standards to facilitate the oversight processes specified in E.O. 14086. NSA also has a Compliance Chief, who provides compliance advice, formal and updated training, and assistance regarding the requirements of E.O. 14086.

FBI's signals intelligence activities are overseen by FBI's Assistant Director of the Inspection Division, Privacy and Civil Liberties Officer, and General Counsel, who work in coordination with appropriate senior officials with data privacy and cybersecurity technical expertise. These activities are also overseen by Department of Justice (DOJ) officials, including DOJ's Inspector General and Assistant Attorney General for the National Security Division.

CIA's signals intelligence activities are overseen by CIA's Inspector General, General Counsel, Privacy and Civil Liberties Officer, and Chief Data Officer, who, in coordination with the Privacy and Civil Liberties Officer, conducts periodic oversight and assessments of data standards, guidelines, and procedures for compliance with the documentation, handling, and retention requirements of E.O. 14086 and conducts periodic audits of compliance with access and training requirements.

These senior-level legal, oversight, and compliance officials meet the above requirements of E.O. 14086, which include ensuring that such officials have access to all information pertinent to carrying out their compliance and oversight responsibilities, that appropriate

[143] *Id.* § 2(d)(i).

actions are taken to remediate an incident of non-compliance, and that such officials are free from actions designed to impede or improperly influence their oversight responsibilities.

Though the remaining IC elements are not subject to this requirement because they do not collect signals intelligence, these elements employ oversight, legal, and compliance officials (e.g., privacy and civil liberties officers, intelligence oversight officials) who are tasked with auditing, reviewing, and overseeing implementation of the Executive Order.

E.O. 14086 also requires that each IC element:

> [E]nsure that, if a legal, oversight, or compliance official . . . or any other employee, identifies a significant incident of non-compliance with applicable United States law, the incident is reported promptly to the head of the element of the [IC], the head of the executive department or agency containing the element of the [IC] (to the extent relevant), and the [DNI].[144]

Significant incidents of non-compliance are defined as:

> [A] systemic or intentional failure to comply with a principle, policy, or procedure of applicable United States law that could impugn the reputation or integrity of an element of the [IC] or otherwise call into question the propriety of an [IC] activity, including in light of any significant impact on the privacy and civil liberties interests of the person or persons concerned.[145]

Examples of significant incidents of non-compliance may include, but are not limited to, an IC element employee releasing classified information to the media or purposefully targeting their family members or friends.[146]

Each IC element's implementing policies and procedures and supplemental guidance require that IC element personnel immediately report potential significant incidents of non-compliance to their chain of command, supervisor, and/or respective agency's legal, oversight, or compliance officials, such as the IC element's Intelligence Oversight Officer, Office of General Counsel (OGC), and/or Office of Inspector General. Personnel at IC elements may also be required to report potential incidents of non-compliance using their respective IC element's incident reporting tool. For instance, potential incidents of non-compliance that are mission-related, such as those related to functions, data, or access, must be reported in NSA's incident reporting tool.[147] The tool is used to capture the information associated with

[144] *Id*. § 2(d)(iii)(A).

[145] *Id*. § 4(l).

[146] Nat'l Sec. Agency, *Identify & Report Questionable Intelligence Activities & Significant or Highly Sensitive Matters*.

[147] *Id*.

the potential non-compliant activity, which is then adjudicated by NSA OGC.[148] Similarly, ODNI's CLPO is in the process of implementing ODNI's Security and Counterintelligence Online Reporting tool, which is an automated tool for reporting, anonymously or with attribution, E.O. 14086-related compliance incidents.[149]

Each report of a potential significant incident of non-compliance will be investigated by the IC element's legal, oversight, or compliance officials to the extent necessary to determine the facts and to assess whether the activity is legal and consistent with applicable policies. If the IC element's legal, oversight, or compliance officials determine that a significant incident of non-compliance has occurred, this incident must be reported promptly to the head of the IC element; the head of the executive department or agency containing the IC element, if applicable; and ODNI.[150] These officials must ensure that any necessary actions are taken to remediate and prevent the recurrence of the significant incident of non-compliance.[151] Though the IC elements did not specify the consequences for significant incidents of non-compliance in their implementing policies and procedures, IC elements confirmed that the consequences may vary based on the severity of the incident and the intentionality of the non-compliance. Therefore, the consequences could range from requiring that an individual complete additional, remedial training on intelligence oversight to removing an individual's access to signals intelligence information.

Any incidents of non-compliance that may be unlawful or contrary to an Executive Order or presidential directive are reported on a quarterly basis to the President's Intelligence Oversight Board, which is a committee of the President's Intelligence Advisory Board, a presidentially appointed advisory body within the Executive Office of the President.[152]

[148] IC Written Responses to PCLOB Questions, at 2 (Feb. 28, 2025).

[149] IC Written Responses to PCLOB Questions, at 6 (Feb. 21, 2025).

[150] E.O. 14086 § 2(d)(iii).

[151] *Id*.

[152] Proclamation No. 13462, 73 Fed. Reg. 11805, §§ 6-8 (Feb. 29, 2008) (amended by Proclamation No. 13516, 744 Fed. Reg, 56621 (Nov. 2, 2009)); Exec. Order No. 12,333 § 1.6(c).

Significant incidents of non-compliance under FISA Section 702 are also reported to congressional oversight committees,[153] DOJ, and the FISC.[154]

As of the date of this report, the IC elements reported to PCLOB that they have not identified any compliance incidents relating to E.O. 14086 since the release of their implementing policies and procedures in 2023.

The Inspectors General for the IC elements are also authorized to evaluate the elements' compliance with the policies and procedures governing their signals intelligence activities.[155] The results of these reviews must be provided to the Attorney General, the DNI, the FISC, and Congress.[156] The Inspectors General of the IC elements have not issued any publicly available reports with respect to E.O. 14086 compliance.[157]

PCLOB assesses that all IC elements have implemented sufficient internal processes to ensure compliance, review, and oversight of signals intelligence activities conducted by IC element personnel.

H. Departures and Deviations

Finally, it should be noted that each IC element included in PCLOB's review allows for departures and deviations from the policies and procedures adopted pursuant to E.O. 14086 in certain circumstances, provided these departures are consistent with the Executive Order

[153] FISA Section 702 mandates congressional oversight, including requiring that the Attorney General provide the Senate Select Committee on Intelligence, the Senate Committee on the Judiciary, the House Permanent Select Committee on Intelligence, and the House Committee on the Judiciary, with a semiannual report that includes copies of the reports from any compliance reviews conducted by DOJ or ODNI and a description of any incidents of non-compliance by the IC reported to the FISC. The congressional committees receive the classified Attorney General and DNI semiannual joint assessment regarding compliance and any reports issued by the Inspectors General. Moreover, the IC elements may promptly notify the congressional intelligence committees of an individual compliance matter, depending on the type of and the severity of the compliance incident. 50 U.S.C. § 1881a, f; *see e.g.,* Nat'l Sec. Agency, *NSA Director of Civil Liberties and Privacy Office Report, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702*, at 3 (2014), https://www.dni.gov/files/documents/0421/702%20Unclassified%20Document.pdf.

[154] IC Written Responses to PCLOB Questions, at 7 (Feb. 21, 2025). For example, the Attorney General and the DNI are tasked with issuing semiannual assessments on compliance with IC elements' targeting, minimization, and querying procedures to the FISC, the congressional intelligence committees, and the Committees on the Judiciary of the House of Representatives and the Senate. *See* 50 U.S.C. § 1881a, f; U.S. Foreign Intel. Surveillance Ct., *FISC Rules of Procedure*, at 5 (2010), https://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.

[155] 50 U.S.C. § 1881a(m)(2).

[156] *Id*.

[157] IC Written Responses to PCLOB Questions, at 2 (March 26, 2025).

and other applicable legal constraints.[158] A similar allowance was made in many IC elements' PPD-28 policies and procedures.[159] While departures from the policies and procedures adopted pursuant to E.O. 14086 must generally be approved in advance by senior IC element officials, each IC element also allows for departures without prior approval in certain exigent circumstances, such as when an "official determines that a departure from these procedures is necessary because of the immediacy or gravity of a threat to the safety of persons or property or to the national security."[160] Each IC element's policies and procedures specify the conditions under which such emergency departures may occur.[161]

As of the date of this report, ODNI confirmed that it has not been notified of any IC element exercising its authority to depart from its E.O. 14086 policies and procedures.

[158] There are a variety of ways in which an IC element could deviate from the policies and procedures it adopted pursuant to E.O. 14086 while still fulfilling its requirements under the Executive Order. For example, and as previously discussed, most IC elements' implementing policies and procedures establish at least some safeguards that go beyond those required under E.O. 14086.

[159] The IC's allowance for departures from both their PPD-28 and E.O. 14086 implementing policies and procedures, either with prior approval or in certain exigent circumstances, is consistent with the Executive Order's requirement that "[t]his order shall apply to signals intelligence activities consistent with the scope of PPD-28's application to such activities prior to PPD-28's partial revocation by the national security memorandum issued concurrently with this order." E.O. 14086 § 5(f).

[160] *NSA/CSS Policy 12-3 Annex C*, *supra*, at C-2.

[161] IC elements' implementing policies and procedures require, among other things, that personnel provide DOJ with prompt notice of any emergency departures stating why advance approval was not possible and describing the actions taken to ensure activities were conducted lawfully. *See e.g.,* Cent. Intel. Agency, *Signals Intelligence Activities*, at 11 (2023); FBI Implementing Policies and Procedures, *supra*, at 9; *NSA/CSS Policy 12-3 Annex C*, *supra*, at C-2.

IV. RECOMMENDATIONS

RECOMMENDATION 1:

IC elements should require regular training on their E.O. 14086 policies and procedures for all personnel with access to signals intelligence information.

E.O. 14086 requires each element of the IC to maintain training requirements to ensure that IC personnel with access to signals intelligence "know and understand" the Executive Order's requirements and the policies and procedures for reporting and remediating incidents of non-compliance with applicable U.S. law. PCLOB has found that the IC elements have fulsome training materials and generally require periodic training of personnel with access to signals intelligence.

When the IC elements initially updated PPD-28 policies and procedures to implement the additional safeguards required by E.O. 14086, some IC elements, such as NRO and CIA, required personnel to retake training within a certain time period. In addition, most IC elements now require that training be completed annually. Pursuant to the access control restrictions mandated by E.O. 14086, access to information collected through signals intelligence activities is restricted to those personnel who have completed their respective IC element's mandatory E.O. 14086 training. Failing that, an individual may be subject to administrative action, such as loss of access to the system and/or signals intelligence data.

Not all IC elements require regular training, which could impact whether or not IC personnel are sufficiently knowledgeable regarding the requirements and safeguards of E.O. 14086 and how those are implemented by their element. This can lead to knowledge gaps and compliance failures. FBI personnel, in particular, while subject to annual training on Section 702, are not subject to periodic E.O. 14086 training requirements after an initial training that is required to gain access to signals intelligence information. All IC elements should require regular, as opposed to one-time, training.

RECOMMENDATION 2:

If IC elements update or change their E.O. 14086 policies and procedures, they should publicly release any updated version, to the maximum extent possible, consistent with the protection of national security.

E.O. 14086 requires IC elements to publicly release, to the maximum extent possible, the policies and procedures they adopted pursuant to the Executive Order "in order to enhance the public's understanding of, and to promote public trust in, the safeguards pursuant to

which the United States conducts signals intelligence activities."[162] Each IC element has complied with this requirement. However, in order to most effectively enhance the public's understanding of, and promote public trust in, E.O. 14086 safeguards, IC elements should also ensure that their publicly available E.O. 14086 policies and procedures are as current as possible. Since IC elements' signals intelligence authorities and practices may change over time, each IC element should (1) periodically review its E.O. 14086 policies and procedures to ensure that they continue to encompass current practices, (2) periodically review its E.O. 14086 practices to ensure that they remain consistent with the Executive Order and the implementing policies, and (3) update its publicly available policies and procedures, consistent with classification requirements, to reflect any pertinent changes in policy and practice.

[162] E.O. 14086 § 2(c)(4).

V. CONCLUSION

This review, the first of two PCLOB planned reports pursuant to E.O. 14086, focused on the implementation of E.O. 14086 through policies and procedures, supplemental guidance, and training adopted by IC elements handling signals intelligence.

Although IC elements' approaches to drafting policies, procedures, and supplemental guidance vary from agency to agency, the agency materials that PCLOB reviewed appropriately implement the Executive Order's requirements. The IC elements have also established oversight mechanisms and staff training requirements designed to support continued compliance. Making public any updates to IC elements' policies and procedures will assist with public transparency, and requiring annual trainings will help ensure continued compliance with the Executive Order.

PCLOB concludes that the IC elements participating in signals intelligence activities have successfully updated their policies and procedures to comply with E.O. 14086 and its requirements. Further, in light of the breadth of requirements, processes, and personnel that the IC elements have instituted pursuant to E.O. 14086 and based on the information available at the time of this report, PCLOB assesses that the IC elements have implemented sufficient internal processes to ensure compliance, review, and oversight of signals intelligence activities consistent with E.O. 14086.