

SAFEGUARDING PERSONAL INFORMATION COLLECTED FROM SIGNALS INTELLIGENCE ACTIVITIES

I. Purpose

This Instruction establishes the policies and procedures governing the safeguarding by Office of Intelligence and Analysis (I&A) personnel of personal information collected from signals intelligence activities as required by Executive Order (E.O.) 14086. Revision 02 supersedes Revision 01 of this Instruction, which implemented Presidential Policy Directive 28.

II. Scope

This Instruction applies to all I&A Personnel, as that term is defined in I&A Instruction IA-1000.

III. References

- A. Title 6, United States Code, Chapter II, Part A, "Information and Analysis; Access to Information."
- B. Executive Order 12333, "United States Intelligence Activities," as amended July 30, 2008.
- C. Executive Order 14086, "Enhancing Safeguards for United States Signals Intelligence Activities," October 7, 2022.
- D. Presidential Policy Directive 28, *Signals Intelligence Activities* (January 17, 2014) (Revoked in Part Pursuant to National Security Memorandum 14).
- E. I&A Instruction IA-1000, "Office of Intelligence and Analysis Intelligence Oversight Program and Guidelines," January 19, 2017.

IV. Definitions

All definitions for this Instruction can be found in IA-1000 and E.O. 14086.

V. Responsibilities

A. The *Under Secretary for Intelligence and Analysis (USIA)*:

1. Establishes policies and procedures that apply the principles for safeguarding personal information collected from signals intelligence activities set forth in E.O. 14086, and ensures that all I&A personnel comply with the requirements of that E.O. and this Instruction;
2. Ensures appropriate measures exist to facilitate oversight of the implementation of safeguards protecting personal information collected from signals intelligence activities;
3. Facilitates the performance of oversight by the Intelligence Oversight Officer and their respective staff, and other relevant oversight entities including the DHS Office for Civil Rights and Civil Liberties, Privacy Office, and Office of General Counsel, as appropriate; and
4. Ensures compliance with any Office of the Director of National Intelligence (ODNI) Civil Liberties Protection Officer (CLPO) determination to undertake appropriate remediation, subject to any contrary determination of the Data Protection Review Court (DPRC), and, further, ensures compliance with any determination by a DPRC panel to undertake appropriate remediation, pursuant to E.O. 14086.

B. The *Intelligence Oversight Officer (IOO)*:

1. Oversees I&A compliance with these policies and procedures;
2. Reports to the USIA regarding the application of the safeguards contained herein and in E.O. 14086, as applicable, as part of their periodic reviews, audits, and reviews of the implementation of these policies;
3. Provides the introductory and periodic training discussed in Section V.C. on the requirements of this Instruction to all I&A personnel who have access to information that is subject to this Instruction;

4. Provides advice and assistance to I&A regarding privacy and civil liberties in implementing these policies and procedures, in consultation with the Chief Privacy Officer and Officer for Civil Rights and Civil Liberties of the Department, as appropriate;
 5. In coordination with the cognizant senior data privacy and information security officials for those systems administered or otherwise utilized by I&A personnel, ensures maintenance of proper data security, access, and quality, to include accreditation of systems that maintain signals intelligence, in accordance with applicable laws, rules, and policies of I&A, the Department, and the IC;
 6. Coordinates with the DHS Office for Civil Rights and Civil Liberties, Privacy Office, and Office of General Counsel on any new or updated procedures for acquiring, handling, or using signals intelligence; and
 7. Executes and implements this Instruction.
- C. The **Director, Intelligence Training Academy**, in coordination with the IOO, the DHS Office for Civil Rights and Civil Liberties, Privacy Office, and Office of the General Counsel, provides training development, delivery, tracking and reporting support, as needed, in compliance with this Instruction and all other applicable laws and policies.
- D. **I&A Personnel** comply with the requirements of this Instruction.

VI. Content and Procedures

- A. **Consistency with Law and Policy**. Pursuant to Section 1.7(i) of E.O. 12333, I&A personnel collect (overtly or through publicly available sources), analyze, produce, and disseminate information, intelligence, and counterintelligence to support national and departmental missions. I&A is not authorized to conduct—and does not conduct—signals intelligence collection activities.
1. **Mission Support Requirement**. I&A personnel retain and disseminate personal information obtained through signals intelligence only to the extent that such information relates to an authorized national or departmental intelligence requirement.
 2. **Privacy and Civil Liberties Safeguards**. The safeguards contained in this section implement the principles contained in subsections (a)(ii) and (a)(iii) of Section 2 of E.O. 14086.

B. **Minimization**. I&A does not have access to unevaluated or unminimized signals intelligence, including signals intelligence collected in bulk, but it may receive, from other intelligence community elements, signals intelligence information that has been evaluated or minimized, including information included in information reports or intelligence products subject to the provisions of Executive Order 14086 among other requirements.¹

1. **Dissemination**. I&A disseminates personal information of non-U.S. persons collected through signals intelligence activities only if dissemination of comparable information concerning U.S. persons would be permitted under Section 2.3 of E.O. 12333. I&A disseminates personal information concerning a non-U.S. person on the basis that it is foreign intelligence only if the information relates to an authorized intelligence requirement and not solely because of the person's foreign nationality or country of residence. Unless it possesses specific information to the contrary, I&A presumes that any evaluated or minimized signals intelligence information it receives from other IC elements that have adopted procedures to implement E.O. 14086 meets this standard. I&A disseminates such 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. I&A takes 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 personal information collected through signals intelligence to recipients outside the U.S. Government, including a foreign government or international organization. Personal information collected through signals intelligence activities is not disseminated for the purpose of circumventing the provisions of E.O. 14086.
2. **Retention**. As required by E.O. 14086, I&A retains personal information of non-U.S. persons collected through signals intelligence activities only if retention of comparable information concerning U.S. persons would be permitted under applicable U.S. law and deletes such information that may no longer be retained in the same manner that comparable information concerning U.S. persons would be deleted. I&A retains personal

¹ References to signals intelligence and signals intelligence activities in this document also apply to intelligence collected and activities conducted pursuant to Section 702 of the Foreign Intelligence Surveillance Act. The sources of or methods of obtaining specific information contained in information reports or intelligence products may not in all cases be evident to I&A or to the Department as a recipient of such reports or products.

information concerning a non-U.S. person on the basis that it is foreign intelligence in accordance with applicable I&A and IC policies and procedures, including its Intelligence Oversight Guidelines, consistent with Section 2(c)(iii)(A)(2) of E.O. 14086, including that information relates to an authorized intelligence requirement and not solely because of the person's foreign nationality or country of residence. Unless it possesses specific information to the contrary, I&A presumes that any evaluated or minimized signals intelligence information it receives from other IC elements that have adopted procedures to implement E.O. 14086 meets this standard. I&A retains such information in accordance with applicable record retention policies and subject it to the same retention periods that would apply to comparable information concerning U.S. persons.

C. **Data Security and Access**

1. **General Requirements.** Access to all personal information collected through signals intelligence activities—irrespective of the nationality of the person whose information is collected—is restricted to those personnel who have a need to access that information in the performance of authorized duties in support of national or departmental missions and have received appropriate training on the requirements of applicable U.S. laws, as implemented by this Instruction and pursuant to E.O. 14086 § 2(c)(iii)(B)(2). Such information is maintained in either electronic or physical form in secure facilities protected by physical and technological safeguards, and with access limited by appropriate security measures. Such information is safeguarded in accordance with applicable laws, rules, and policies, including those of I&A, the Department, and the IC.
 2. **Classified Information.** Classified information is stored appropriately in a secured, certified, and accredited facility, in secured databases or containers, and in accordance with other applicable requirements. I&A's electronic system in which such information may be stored complies with applicable law, Executive Orders, and IC and Department policies and procedures regarding information security, including with regard to access controls and monitoring.
- D. **Data Quality.** Personal information collected through signals intelligence activities – where such information can be so identified – is included in I&A intelligence products only as consistent with applicable IC standards of analytic tradecraft, including such standards for accuracy and objectivity, as set forth in relevant directives, including Intelligence Community Directive 203, *Analytic Standards*. Particular care should be taken to apply standards relating to the relevance, quality, and reliability of the information,

consideration of alternative sources of information and interpretations of data, and objectivity in performing analysis.

E. **Oversight**

1. **Periodic Review.** The IOO, in consultation with the Associate General Counsel for Intelligence, reviews implementation of this Instruction periodically, focusing particularly on relevant portions of E.O. 14086 regarding privacy and civil liberties, and reports to the USIA regarding the application of the safeguards contained herein and in E.O. 14086 more generally, as applicable. The IOO briefs their findings, provides copies of review reports to the Department's Chief Privacy Officer and Officer for Civil Rights and Civil Liberties, and, as appropriate, consults with these offices on responsive steps to remediate any concerns identified through the reviews. The IOO serves as the primary point of contact with the Privacy and Civil Liberties Oversight Board regarding E.O. 14086 compliance and coordinates any such activity with the Department's Chief Privacy Officer. I&A, through the IOO, will develop an audit and compliance review procedure within one year of the effective date of this Instruction. I&A personnel are required to support any such reviews to the maximum extent possible.
 2. **Instances of Non-Compliance.** I&A personnel report instances of non-compliance with this Instruction to the IOO, who, in consultation with the Associate General Counsel for Intelligence, promptly reports instances of non-compliance to relevant entities to ensure their remediation and promptly reports significant instances of non-compliance with applicable U.S. law (i.e., systemic or intentional failures 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 Intelligence Community or otherwise call into question the propriety of an Intelligence Community activity, including in light of any significant impact on the privacy and civil liberties interests of the person or persons concerned) involving the personal information of any person collected through signals intelligence activities to the USIA, the Secretary of Homeland Security, and the Director of National Intelligence, consistent with Section 2(d)(iii) of E.O. 14086. The IOO also provides notice of significant instances of non-compliance to the Department's Chief Privacy Officer and Officer for Civil Rights and Civil Liberties.
- F. **Assistance to the ODNI Civil Liberties Protection Officer.** I&A, through the IOO, provides the ODNI CLPO with access to information necessary to conduct the reviews described in either Section 3(c)(i) or Section 3(d)(i) of E.O. 14086, consistent with the protection of intelligence sources and methods. I&A personnel do not take any action designed to impede or

improperly influence the ODNI CLPO's review of qualifying complaints or the DPRC's review of the ODNI CLPO's determination of such pursuant to the Signals Intelligence Redress Mechanism.

G. Assistance to the Privacy and Civil Liberties Oversight Board (PCLOB).

I&A, through the IOO, provides the PCLOB with access to information necessary to conduct the reviews described in Section 3(e)(i) of E.O. 14086, in consultation or coordination with Department's Chief Privacy Officer, as appropriate and consistent with the protection of intelligence sources and methods.

H. Training. All I&A personnel who have access to information that is subject to this Instruction will receive introductory and periodic training on applicable requirements, including reporting procedures. Successful completion of such training is a prerequisite to initial and continued access. I&A, through coordination between the IOO and the Director, ITA, monitors completion of training requirements to ensure compliance with this provision.

I. Deviations from these Procedures. Deviations from this Instruction are permitted only in accordance with the requirements set forth below.

1. **Prior Approval.** The USIA must approve in advance any departures from these procedures, after consultation with the Director of National Intelligence and the Assistant Attorney General for National Security, following consultation with the Associate General Counsel for Intelligence.
2. **Exigent Circumstances.** If there is not time for prior approval and consultation and a departure from the procedures in this Instruction is necessary because of the immediacy or gravity of a threat to the safety of persons or property, or to the national security, the USIA or their designee may approve a departure from these procedures.
3. **Notification.** The USIA or their designee reports any departures from the substantive provisions of this Instruction, pursuant to Section V.I.2 of the Instruction, to the Associate General Counsel for Intelligence and, through the Intelligence Oversight Officer, to the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties as soon after the departure as possible. Such notification includes a brief explanation as to why exigent circumstances warranted the departure. Additionally, the Associate General Counsel for Intelligence provides prompt written notice of any such departures stating why advance approval was not possible and describing the actions taken to ensure activities were conducted lawfully to

the Director of National Intelligence and the Assistant Attorney General for National Security.

4. **Lawfulness Required**. Notwithstanding the provisions for amendment or departure set forth above, all I&A intelligence activities must be carried out in a manner consistent with the Constitution and laws of the United States, including the requirements of Executive Orders 12333 and 14086.

- J. **Internal Guidance and Interpretation**. These procedures are set forth solely for internal guidance within I&A. Questions on the applicability or interpretation of these procedures should be directed to the Associate General Counsel for Intelligence, who determines such applicability or interpretation, in consultation with the Department of Justice, as appropriate.

VII. Office of Primary Responsibility

The office of primary responsibility for this Instruction is the Transparency and Oversight Program Office.


Kenneth L. Wainstein
Under Secretary for Intelligence and Analysis

29 June 23
Date