

UNCLASSIFIED

Executive Order 14086 Implementing Policy and Procedures

**DEPARTMENT OF ENERGY
OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE**

**DOE-IN POLICY GUIDANCE
NUMBER 28.2**



**U.S. DEPARTMENT OF
ENERGY**

**Intelligence and
Counterintelligence**

**POLICY AND PROCEDURES IMPLEMENTING EXECUTIVE ORDER 14086
REGARDING USE, MAINTENANCE AND HANDLING OF SIGNALS
INTELLIGENCE INFORMATION
(Effective: June 27, 2023)**

- A. INTRODUCTION:** Executive Order (E.O.) 14086, *Enhancing Safeguards for United States Signals Intelligence Activities* (October 7, 2022), bolsters privacy and civil liberty safeguards for U.S. signals intelligence activities and creates an independent and binding mechanism enabling individuals in qualifying states (defined as countries and regional economic integration organizations), as designated under the E.O., to seek redress through the submission of a qualifying complaint if they believe their personal data was collected through U.S. signals intelligence in a manner that violated applicable U.S. law. Among other provisions, Section 2(c)(iv) of E.O. 14086 requires the head of each element of the Intelligence Community (IC) to: continue to apply relevant policies and procedures issued pursuant to Presidential Policy Directive 28 of January 17, 2014; update those policies and procedures as necessary to implement the privacy and civil liberties safeguards in E.O. 14086; and release the updated policies and procedures publicly to the maximum extent possible.

This document constitutes the updated policies and procedures of the Department of Energy, Office of Intelligence and Counterintelligence (DOE-IN). DOE-IN is an element of the IC pursuant to Section 3 of the National Security Act of 1947, as amended, and Section 3.5(h) of E.O. 12333, as amended.

DOE-IN provides all-source intelligence analysis and information to support the Secretary of Energy and other Department officials and is responsible for all intelligence and counterintelligence activities throughout the DOE complex, including nearly thirty intelligence and counterintelligence offices nationwide. DOE-IN protects vital national security information and technologies, representing intellectual property of incalculable value; provides leading-edge, scientifically-based and technically-sound foreign nuclear and energy security intelligence analysis that enables U.S. policy makers to address critical national security issues; serves in a liaison capacity for DOE with the IC and represents the

UNCLASSIFIED

Department in a variety of intelligence-related fora; and manages and operates the Department's Top Secret/Sensitive Compartmented Information network.

- B. AUTHORITY:** Pursuant to Section 1.7(i) of E.O. 12333, as amended, DOE-IN is to "[c]ollect (overtly or through publicly available sources), analyze, produce, and disseminate information, intelligence, and counterintelligence to support national and departmental missions."

DOE-IN is not authorized to conduct – and does not conduct – signals intelligence collection activities. However, DOE-IN is authorized to receive intelligence reporting containing signals intelligence from other IC agencies authorized to collect such intelligence.

- C. PURPOSE:** This policy guidance replaces DOE-IN Policy Guidance 28.1, *Implementation of PPD-28*, and updates DOE-IN's policies and procedures related to the use, maintenance, and handling of signals intelligence information. This policy guidance fulfills the necessity and proportionality requirements of E.O. 14086, Section 2(a)(ii)-(iii).
- D. APPLICABILITY:** This policy guidance applies to all components of DOE-IN including Headquarters, Field Intelligence Elements, and Counterintelligence Field Offices. These policies and procedures shall be used by all DOE-IN employees and contractors, and employees of other elements or departments who are detailed to DOE-IN and perform DOE-IN work under the direction and supervision of DOE-IN.
- E. PROCEDURES TO SAFEGUARD PERSONAL INFORMATION COLLECTED THROUGH SIGNALS INTELLIGENCE:** The following policies and procedures apply to DOE-IN's safeguarding of personal information of non-U.S. persons collected through signals intelligence activities.¹

1. **Minimization.** DOE-IN does not access unevaluated, raw, or unminimized signals intelligence under DOE authorities, including signals intelligence collected in bulk. However, it may receive, from other IC elements, signals intelligence information² that has been evaluated, minimized, or otherwise included in finished intelligence products subject to – among other requirements – the provisions of E.O. 14086.
2. **Dissemination.** DOE-IN will disseminate 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 and the Attorney General approved guidelines, the

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. These procedures do not alter the rules applicable to U.S. persons found in the Foreign Intelligence Surveillance Act, E.O. 12333, DOE-IN's guidelines approved by the Attorney General pursuant to Sec. 2.3 of E.O. 12333, or other applicable law.

² Absent signals intelligence classification caveats or warnings, whether an evaluated or finished intelligence product received from another intelligence agency contains signals intelligence is sometimes unknown.

DOE Procedures for Intelligence Activities. DOE-IN will disseminate personal information concerning a non-U.S. person on the basis that it is foreign intelligence or counterintelligence 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, DOE-IN will presume that any evaluated or minimized signals intelligence information it receives from other IC elements that have adopted procedures to implement E.O. 14086 meets these standards. DOE-IN shall disseminate within the U.S. 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. DOE-IN shall 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 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 will not be disseminated for the purpose of circumventing the provisions of E.O. 14086. For purposes of these policies and procedures, "dissemination" shall mean the transmission, communication, sharing, or passing of information outside of DOE-IN by any means, including oral, electronic, or physical.

3. **Retention and Deletion.** DOE-IN will retain 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 law and the *DOE Procedures for Intelligence Activities*. DOE-IN will retain personal information concerning a non-U.S. person on the basis that it is foreign intelligence or counterintelligence in accordance with applicable DOE-IN policies and procedures, consistent with Section 2(c)(iii)(A)(2) of E.O. 14086, including that information relate to an authorized intelligence requirement and not be retained solely because of the person's foreign nationality or country of residence. Unless it possesses specific information to the contrary, DOE-IN will presume that any evaluated or minimized signals intelligence information it receives from other IC elements that have adopted procedures to implement E.O. 14086 meets these standards. DOE-IN will retain such information in accordance with applicable record retention policies and shall subject it to the same retention periods that would apply to comparable information concerning U.S. persons. Non-U.S. person information collected through signals intelligence that does not meet the threshold for retention by DOE-IN, will be deleted in accordance with deletion policy standards and procedures for USPI consistent with E.O. 14086 Section 2(c)(iii)(A)(2)(c). For purposes of these policies and procedures, "retention" shall mean the maintenance of signals intelligence containing non-U.S. person information in either hard copy or electronic format.

4. **Data Access and Security.** 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 DOE-IN or Department missions. Such information will be 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 will be safeguarded in accordance with applicable laws, rules, and policies, including those of DOE-IN, the Department, and the IC.

Classified information will be stored appropriately in a secured, certified, and accredited facility, in secured databases or containers, and in accordance with other applicable requirements. DOE-IN's electronic system in which such information may be stored will comply with applicable law, Executive Orders, and IC and Department policies and procedures regarding information security, including with regard to access controls and monitoring.

The DOE-IN Chief Information Officer and DOE-IN Chief Information Security Officer, in consultation with the DOE-IN Civil Liberties and Privacy Officer (CLPO) and DOE Assistant General Counsel for International and National Security Programs (GC-74), will ensure that the electronic systems in which signals intelligence information is stored are certified under and adhere to established standards.

5. **Data Quality.** Personal information collected through signals intelligence activities – where such information can be so identified – shall be included in DOE-IN 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.

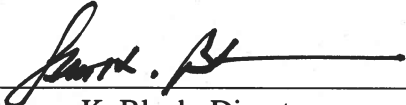
- F. OVERSIGHT:** The DOE-IN CLPO shall review implementation of these policies and procedures annually, focusing particularly on relevant provisions of E.O. 14086 regarding privacy and civil liberties, and shall report to the Director, DOE-IN regarding the application of the safeguards contained herein and in E.O. 14086 more generally, as applicable.

All DOE-IN personnel should report potential instances of non-compliance with these policies and procedures to the DOE-IN CLPO. The DOE-IN CLPO, in coordination with GC-74, shall promptly report instances of non-compliance to relevant entities to ensure their remediation, consistent with existing reporting requirements under applicable law, regulation, Presidential direction, and policy. Should the DOE-IN CLPO, in coordination with GC-74, determine that an incident of non-compliance is a “significant incident of non-compliance” as defined in Section of 4 of E.O. 14086, the DOE-IN CLPO shall promptly report it to the

Director, DOE-IN, and the Director of National Intelligence, who shall ensure that any necessary actions are taken to remediate it and prevent its recurrence and shall further ensure that any other relevant officials are notified, as appropriate.

- G. TRAINING:** DOE-IN personnel whose duties require access to information collected through signals intelligence activities will receive annual training on the requirements of these policies and procedures. Successful completion of such training is a prerequisite to initial and continued access, and DOE-IN will monitor completion of training requirements to ensure compliance with this provision.
- H. ASSISTANCE TO THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE CIVIL LIBERTIES AND PRIVACY OFFICER (ODNI CLPO):** DOE-IN components shall provide 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. DOE-IN personnel shall not take any action designed to impede or improperly influence the ODNI CLPO's review of qualifying complaints, or the Data Protection Review Court's review of the ODNI CLPO's determination of such pursuant to the Signals Intelligence Redress Mechanism. DOE-IN components shall comply with any ODNI CLPO determination to undertake appropriate remediation, subject to any contrary determination by the Data Protection Review Court, and further, shall comply with any determination by a Data Protection Review Court panel to undertake appropriate remediation.
- I. ASSISTANCE TO THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD:** DOE-IN components shall provide the Privacy and Civil Liberties Oversight Board with access to information necessary to conduct the annual review of the signals intelligence redress mechanism described in Section 3(e) of E.O. 14086, consistent with the protection of intelligence sources and methods.
- J. DEVIATIONS FROM THESE PROCEDURES:** The Director, DOE-IN together with GC-74 must approve in advance any departures from these procedures, after consultation with ODNI and the National Security Division of the Department of Justice. If there is not time for such approval and 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, the Director, DOE-IN may approve a departure from these procedures. GC-74 will be notified as soon thereafter as possible. DOE-IN will also provide 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 ODNI and the National Security Division of the Department of Justice. Notwithstanding this paragraph, all activities in all circumstances must be carried out in a manner consistent with the Constitution and laws of the United States, and E.O. 12333 and E.O. 14086.
- K. INTERPRETATION:** These procedures are set forth solely for internal guidance within DOE-IN. Questions on the applicability or interpretation of these procedures should be directed to the DOE-IN CLPO, who shall determine such applicability or interpretation, in consultation with GC-74, as appropriate.

L. EFFECTIVE DATE: This policy is effective upon signature.
SIGNATURE AND DATE.



Steven K. Black, Director
Office of Intelligence and Counterintelligence
Department of Energy

June 27, 2023
Date