DEPARTMENT OF ENERGY
OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE

DOE-IN POLICY GUIDANCE
NUMBER 28.1

U.S. DEPARTMENT OF ENERGY | Intelligence and Counterintelligence

IMPLEMENTATION OF PPD-28
(Effective: 16 JANUARY 2015)

A. SUMMARY: This document describes the Office of Intelligence and Counterintelligence (DOE-IN) policy for safeguarding personal information collected through signals intelligence.

B. AUTHORITY: Presidential Policy Directive 28, *Signals Intelligence Activities* (hereinafter "PPD-28"), issued 17 January 2014, articulates principles to guide why, whether, when, and how the United States conducts signals intelligence activities for authorized foreign intelligence and counterintelligence purposes. Specifically, PPD-28 § 4 sets forth principles for safeguarding personal information collected from signals intelligence activities and requires Intelligence Community (IC) elements to establish policies and procedures to apply such principles, consistent with technical capabilities and operational needs.

DOE-IN is an element of the IC pursuant to the National Security Act of 1947 § 3, as amended, and Executive Order 12333 § 3.5(h), as amended.

Pursuant to Executive Order 12333 § 1.7(i), 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."

In addition, pursuant to Executive Order 12333 § 1.12, as amended, the Secretary of Energy shall, "Provide expert scientific, technical, analytic, and research capabilities to other agencies within the Intelligence Community, as appropriate."

DOE-IN conducts these activities in accordance with the Department of Energy Procedures for Intelligence Activities ("DOE Procedures"), approved by the Attorney General under Executive Order 12333 on 19 October 1992.

Pursuant to the DOE Procedures, DOE-IN is not authorized to independently conduct signals intelligence collection. DOE-IN is, however, authorized to support authorized foreign intelligence and counterintelligence collection activities of other IC elements. In the event DOE-IN is requested to support signals intelligence collection activities of other IC elements, DOE-IN conducts those support activities in accordance with the approved intelligence procedures of the requesting agency, to include the requesting agency's PPD-28 policies and procedures.

C. **PURPOSE:** This document provides specific guidance on the implementation of PPD-28, *Signals Intelligence Activities*. This policy guidance is adopted in order to ensure appropriate safeguards for the personal information of all individuals, regardless of the nationality of the individual to whom the information pertains or where the individual resides.

D. **APPLICABILITY:** This policy guidance applies to DOE-IN's safeguarding of personal information of non-U.S. persons collected through signals intelligence activities.[1]

These procedures are set forth solely for internal guidance within DOE-IN. Questions regarding the applicability or interpretation of these procedures should be directed to the Director of the Office of Intelligence and Counterintelligence, who shall determine such applicability or interpretation, in consultation with the advising legal office, as appropriate.

E. **PROCEDURES TO SAFEGUARD PERSONAL INFORMATION COLLECTED THROUGH SIGNALS INTELLIGENCE.**

1. **Minimization.** DOE-IN does not have access to raw or unminimized signals intelligence, including signals intelligence collected in bulk, but it receives, from other IC elements, signals intelligence information[2] that has been minimized or otherwise included in finished intelligence products subject to—among other requirements—the provisions of PPD-28.[3]
   a) **Dissemination.** DOE-IN will disseminate personal information concerning a non-U.S. person collected through signals intelligence activities only if dissemination of comparable information concerning U.S. persons would be

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

[2] The origins of specific information contained in evaluated or finished intelligence products—or the specific means by which such information was collected—may not in all cases be evident to DOE-IN or DOE as a recipient of such intelligence products.

[3] Such PPD-28 provisions include those in Section 1, such as (i) the United States shall not collect signals intelligence for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion; (ii) signals intelligence shall be collected exclusively where there is a foreign intelligence or counterintelligence purpose to support national and departmental missions and not for any other purposes; (iii) it is not an authorized foreign intelligence or counterintelligence purpose to collect foreign private commercial information or trade secrets to afford a competitive advantage to U.S. companies and U.S. business sectors commercially; and (iv) signals intelligence activities shall be as tailored as feasible. If DOE-IN identifies signals intelligence disseminated to DOE-IN that it believes may have been collected in a manner that is not consistent with PPD-28, it shall so notify appropriate officials at the IC element that collected the information.

permitted under Executive Order 12333 § 2.3, the DOE Procedures and applicable IC policies. DOE-IN will disseminate personal information concerning a non-U.S. person that is foreign intelligence only if the information relates to an authorized intelligence requirement and not solely because of the person's foreign status. Unless it possesses specific information to the contrary, DOE-IN will presume that any signals intelligence information it receives from other IC elements meets these standards. DOE-IN will disseminate such information in accordance with applicable DOE-IN and IC policies and procedures.

b) **Retention.** 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 Executive Order 12333 § 2.3, the DOE Procedures and applicable IC policies. DOE-IN will retain personal information concerning a non-U.S. person that is foreign intelligence only if the information relates to an authorized intelligence requirement and not solely because of the person's foreign status. Unless is possesses specific information to the contrary, DOE-IN will presume that any evaluated or minimized signals intelligence information it receives from other IC elements meets this standard. DOE-IN will retain such information in accordance with applicable record retention policies.

2. **Data Security and Access.** 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 IC 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, DOE, 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 DOE policies and procedures regarding information security, including with regard to access controls and monitoring.

3. **Data Quality.** Personal information of both U.S. and non-U.S. persons collected through signals intelligence activities—when identifiable—shall be included in DOE-IN intelligence products only as consistent with applicable DOE Procedures and IC standards of analytic tradecraft as set forth in relevant IC directives.

4. **Oversight.** DOE-IN shall review implementation of these policies and procedures regarding the application of the safeguards contained herein and in PPD-28 § 4 more generally, as applicable.

   Instances of non-compliance with these policies and procedures shall be reported to the Director or a designee. DOE-IN shall ensure that it makes available to its workforce information on how DOE-IN personnel may securely report violations of law, rule or regulation. Each report of questionable activity shall be investigated to the extent necessary to determine the facts and assess whether the activity is legal and consistent with applicable policy. The officials responsible for these investigations may, in accordance with established procedures, obtain assistance from the component concerned, or from other DOE components as necessary to complete the investigations in a timely manner.

   Significant instances of non-compliance with these policies and procedures involving the personal information of any person, regardless of nationality, collected through signals intelligence activities must be reported promptly to the Director and the DNI pursuant to PPD-28 § 4.

F. **TRAINING:** DOE-IN personnel whose duties require access to personal 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 perquisite to access such information.

G. **DEVIATIONS FROM THESE PROCEDURES:** The Director must approve, in advance, of any departures from these procedures after consultation with the Office of the Director of National Intelligence 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 or designee may approve a departure from these procedures. The Director and the appropriate legal adviser will be notified as soon thereafter as possible. DOE-IN will provide prompt written notice of any such departures to the Office of the Director of National Intelligence and the National Security Division. 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.

H. **EFFECTIVE DATE:** This policy guidance is effective upon signature.

I. SIGNATURE AND DATE.

Steven K. Black **Director** **Office of Intelligence and Counterintelligence** **Department of Energy**	1/16/15 **Date**