U.S. Department of State
Bureau of Intelligence and Research
Executive Order 14086 – Policy and Procedures

I. Introduction

Executive Order (E.O.)14086 of October 7, 2022, on Enhancing Safeguards for United States Signals Intelligence Activities, 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 the E.O. 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 the E.O.; and release the updated policies and procedures publicly to the maximum extent possible.

This document constitutes the updated policies and procedures of the Bureau of Intelligence and Research (INR). INR is a bureau of the U.S. Department of State (the "Department") and also 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.

INR provides all-source intelligence analysis and information to support the Secretary of State, U.S. diplomats, and other Department officials; coordinates policymaker use of IC information in foreign engagements and public diplomacy; ensures that intelligence activities support foreign policy and national security purposes; serves as the focal point in the Department for facilitating policy review of covert action, sensitive intelligence,

counterintelligence, and law enforcement activities; serves in a liaison capacity for the Department with the IC and represents the Department in a variety of intelligence-related fora; and manages and operates the Department's Top Secret/Sensitive Compartmented Information network.

II. General Provisions and Authorities

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

INR is not authorized to conduct – and does not conduct – signals intelligence activities. [1]

III. Safeguarding Personal Information Collected through Signals Intelligence

The following policies and procedures fulfill the principles contained in Section 2(a)(ii)-(iii) of E.O. 14086 and apply to INR's safeguarding of personal information of non-U.S. persons collected through signals intelligence activities conducted by IC agencies who are authorized to collect signals intelligence.[2] These policies and procedures do not apply to information collected through diplomatic reporting.

These policies and procedures shall be used by all INR employees and contractors, employees of other departments or agencies who are detailed to INR and perform INR work under the direction and supervision of INR, and any other State Department employees when they are performing intelligence activities authorized pursuant to E.O.12333 (collectively, "INR personnel").

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

A. Minimization

INR does not have access to unevaluated, raw, or unminimized signals intelligence, including signals intelligence collected in bulk, but it receives, from other IC elements, signals intelligence information[3] that has been evaluated, minimized, or otherwise included in finished intelligence products subject to – among other requirements – the provisions of E.O. 14086. Unless it possesses specific information to the contrary, INR will presume that any evaluated or minimized signals intelligence information it receives from other IC elements that have adopted procedures implementing E.O. 14086 and which has been disseminated is consistent with that Executive Order.

i. Dissemination

In limited situations where INR receives personal information of non-U.S. persons collected through signals intelligence activities, it will only disseminate such information if dissemination of comparable information concerning U.S. persons would be permitted under Section 2.3 of E. O. 12333.

INR will disseminate personal information collected through signals intelligence on the basis that it is foreign intelligence only if the information relates to an authorized intelligence requirement and not solely because of a person's nationality or country of residence. INR will disseminate within the U.S. Government personal information concerning a non-U.S. person that is foreign 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. INR 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

[3] The sources of or methods of obtaining specific information contained in evaluated or finished intelligence products may not in all cases be evident to INR or to the Department as a recipient of such intelligence products.

U.S. government, including to a foreign government or international organization. INR shall not disseminate personal information collected through signals intelligence for the purpose of circumventing the provisions of E.O. 14086.

For purposes of these policies and procedures, "dissemination" means the transmission, communication, sharing, or passing of information outside of INR by any means, including oral, electronic, or physical.

ii. Retention

INR 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 U.S. law. INR will retain personal information concerning a non-U.S. person that is foreign intelligence in accordance with applicable Bureau and IC policies and procedures, consistent with Section 2(c)(iii)(A)(2) of E.O. 14086, including that information relates to an authorized intelligence requirement and not be retained solely because of the person's foreign nationality or country of residence. INR will retain personal information concerning a non-U.S. person under the same retention periods and manner of deletion that would apply to comparable information concerning U.S. persons. If INR retains personal information of a non-U.S. person because it is foreign intelligence, the information must relate to an authorized intelligence requirement, and cannot be retained solely because of the non-U.S. person's foreign status.

B. Data Security and Access

Access to all personal information collected through signals intelligence activities – irrespective of the nationality or country of residence of the person whose information is collected – is restricted to authorized and appropriately trained personnel who

have a need to access that information in the performance of authorized duties. 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 INR, 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. The Chief Information Officer and Chief Information Security Officer for INR, in consultation with the Privacy and Civil Liberties Officer and Office of the Legal Adviser, as appropriate, will ensure that the electronic systems in which signals intelligence information is stored are certified under and adhere to established standards. Such electronic systems 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.

C. Data Quality

Personal information collected through signals intelligence activities – when identifiable – shall be included in INR intelligence products only as consistent with applicable IC standards of analytic tradecraft as set forth in relevant IC directives, including ICD 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.

D. Oversight

The Assistant Secretary of INR, or his or her designee, shall review implementation of these policies and procedures annually, focusing particularly on relevant provisions of E.O. 14086 regarding privacy and civil liberties.

Instances of non-compliance with these policies and procedures shall be reported to the INR Civil Liberties, Privacy and Transparency Officer, who, in consultation with the Office of the Assistant Legal Adviser for Law Enforcement and Intelligence, shall determine what corrective actions are necessary, if any. In addition, all INR personnel are required to report criminal activity, including fraud, waste, and abuse involving IC activities, operations, programs, or personnel to the Office of the Inspector General of the Intelligence Community. INR personnel may also report other potential instances of non-compliance with U.S. law, these policies and procedures, or other matters of concern to the IC IG.

Significant instances of non-compliance with applicable U.S. law involving the personal information of any person collected through signals intelligence activities shall be reported promptly to the Assistant Secretary, the Secretary of State, and the Director of National Intelligence, consistent with Section 2(d)(iii) of E.O. 14086.

E. Assistance to the Signals Intelligence Redress Mechanism

INR shall provide the Civil Liberties and Privacy Officer for the Office of the Director of National Intelligence (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. INR 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 review of the CLPO's determination of such pursuant to the Signals Intelligence Redress Mechanism. INR shall comply with any determination by the ODNI CLPO to undertake appropriate remediation, subject to any contrary determination by the Data Protection Review Court, and, further shall comply with any determination of a Data Protection Review Court panel to undertake appropriate remediation. INR 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.

IV. Training

INR personnel whose duties require access to information collected through signals intelligence activities will receive annual training on the requirements of these policies and procedures. INR will monitor completion of training requirements to ensure compliance with this provision.

V. Deviations from these Procedures

The Assistant Secretary must approve in advance 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 Assistant Secretary, or the Assistant Secretary's senior representative present, may approve a departure from these procedures. The Assistant Secretary and the Office of the Legal Adviser will be notified as soon thereafter as possible. The Office of the Legal Adviser will 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 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.

VI. Conclusion

These procedures are set forth solely for internal guidance within INR. Questions on the applicability or interpretation of these procedures should be directed to the Assistant Secretary, who shall determine such applicability or interpretation, in

consultation with the Office of the Assistant Legal Adviser for Law Enforcement and Intelligence, as appropriate.

Approved: [signature]

Date: 6-29-2023