NATIONAL RECONNAISSANCE OFFICE
14675 Lee Road
Chantilly, VA 20151-1715

Office of the Director Policy Note

Number 2023-04 **27 June 2023**

EXECUTIVE ORDER 14086 - ENHANCING SAFEGUARDS FOR UNITED STATES SIGNALS INTELLIGENCE ACTIVITIES

I. Introduction

Executive Order 14086 of 7 October 2022, *Enhancing Safeguards for United States Signals Intelligence Activities*, (EO 14086) was issued to set forth principles and safeguards to guide the conduct of signals intelligence to provide national security decision makers timely, accurate, and insightful information necessary to advance the national security interests of the United States (U.S.) while also ensuring the dignity and respect of all persons and safeguarding their legitimate privacy and civil liberty interests in the handling of their personal information, regardless of their nationality or where they reside.

EO 14086 further establishes a redress mechanism to review qualifying complaints of signals intelligence activities conducted in violation of U.S. law.

EO 14086 also requires all Intelligence Community (IC) elements to update policies previously issued pursuant to Presidential Policy Directive 28 (PPD 28) of 17 January 2014 (*Signals Intelligence Activities*) in accordance with the requirements published in EO 14086.

This Policy Note constitutes the updated PPD 28 policies and procedures as required by EO 14086; supersedes and rescinds Policy Note 2015-01, dated 23 January 2015; and will serve as the basis for any future related NRO instructions.

II. General Provisions and Authorities

NRO is a Defense Agency and an element of the IC pursuant to Section 3.5(h) of Executive Order 12333 (EO 12333), as amended.

Pursuant to Section 1.7(d) of EO 12333, as amended, NRO is to "be responsible for research and development, acquisition, launch, deployment, and operation of overhead systems and related data processing facilities to collect intelligence and information to support national and departmental missions and other United States Government needs."

NRO delivers intelligence, surveillance, and reconnaissance capabilities; information products; services; and tools in response to national-level tasking in coordination with the Functional Managers. NRO provides collection capabilities and related data processing in support of IC, Department of Defense (DoD), and other U.S. Government (USG) needs. While the NRO does not collect or produce signals intelligence it does have access to unevaluated and unminimized RF data, which it transfers to the National Security Agency (NSA) to produce signals intelligence or have access to unevaluated signals intelligence with personal information including that collected in bulk, additionally, the NRO does provide support to other IC elements to facilitate their collection of signals intelligence. NRO conducts RDT&E of signals data, also known as radio frequency data, to support its authorized mission, including the operation of its overhead systems. NRO conducts these activities to enhance the National Security Agency's (NSA) signals intelligence capabilities for further processing, evaluation, and minimization in accordance with NSA procedures. In addition, NRO receives signals intelligence from other IC elements that has been evaluated, minimized, appropriately tagged for cataloguing, or otherwise included in finished intelligence products subject to - among other requirements - the provisions of EO 14086.

III. Safeguarding Personal Information Collected through Signals Intelligence

The following policies and procedures apply to NRO's safeguarding of personal information of non-U.S. persons collected through signals intelligence activities.[1] These safeguards fulfill the principles contained in Section 2(a) of EO 14086.

a. Minimization

Although NRO has access to unevaluated and unminimized signals intelligence, it transfers such data to NSA for processing, evaluation, and minimization in accordance with NSA procedures under the auspices of the Overhead Collection Management Center, an IC-chartered Joint Center. Additionally, NRO receives disseminated signals intelligence information - including personal information - collected by other IC elements that has been evaluated, minimized, or otherwise included in finished intelligence products subject to, among other legal and policy requirements, the provision of EO 14086. Unless it possesses specific information to the contrary, NRO will presume that any evaluated or minimized signals intelligence information it receives from other IC elements that have adopted procedures implementing EO 14086 meets this standard.

[1] These procedures do not alter the rules applicable to U.S. persons found in the Foreign Intelligence Surveillance Act (FISA), EO 12333, or other applicable law. References to signals intelligence and signals intelligence activities in this document also apply to information in finished intelligence products potentially derived from FISA 702 information.

SUBJECT: EXECUTIVE ORDER 14086 - ENHANCING SAFEGUARDS FOR UNITED STATES SIGNALS INTELLIGENCE ACTIVITIES

NRO will apply the following policies and procedures for safeguarding personal information collected through signals intelligence. These policies shall fulfill the principles contained in subsections 2(a)(ii) and 2(a)(iii) of the EO 14086.

1. Dissemination

Consistent with EO 12333, NRO does not produce nor disseminate finished foreign intelligence or counterintelligence products. For purposes of these policies and procedures, "dissemination" shall mean the transmission, communication, sharing, showing, or passing of information outside of NRO by any means, including oral, electronic, or physical means or by providing another entity with access to an NRO information system.[2]

NRO components 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 EO 12333. Under no circumstance will NRO components disseminate personal information of any person solely on the basis of that person's nationality or country of residence. NRO components shall take due account of the conditions for dissemination outside of the USG contained in Section 2(c)(iii)(A)(1)(d) of EO 14086 before disseminating personal information collected through signals intelligence to recipients outside the USG, including to a foreign government or international organization.

NRO components shall disseminate within the USG such signals intelligence information 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. Dissemination of such information must be only in accordance with applicable executive orders, agreements, and policies and procedures of the supported USG entity.

Personal information collected through signals intelligence shall not be disseminated for the purpose of circumventing any of the requirements of EO 14086.

2. Retention

For purposes of these policies and procedures, "retention" shall mean the maintenance of personal information in either hard copy or electronic format regardless of how the information was collected.

NRO will retain personal information of non-U.S. persons collected through signals intelligence activities only if retention of

[2] This definition of "dissemination" is taken from DoD Manual 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*. These are the Attorney General approved procedures applicable to NRO.

comparable information concerning U.S. persons would be permitted under Section 2.3 of EO 12333 and other applicable law, executive orders, and policies and procedures. NRO will retain 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 non-U.S. person status. Personal information of non-U.S. persons information that may no longer be retained shall be deleted in the same manner as comparable information concerning U.S. persons would be deleted.

b. Data Security and Access

NRO Components will maintain all personal information of non-U.S. persons collected through signals intelligence activities under the same data security and access standards applied to equivalent personal information of U.S. persons. The Chief Information Officer and Chief Information Security Officer, in consultation with the NRO Privacy and Civil Liberties Program Office (PCLPO) and OGC, will ensure that NRO systems in which signals intelligence information is stored are certified under and adhere to established standards.

Access to personal information collected through signals intelligence activities - when identifiable - is restricted to those personnel who have a need to know that information in the performance of authorized duties in support of NRO's mission and have satisfied applicable training requirements. 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, executive orders, agreements, rules, and policies and procedures, including those of NRO, the DoD, 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 NRO electronic system in which such information may be stored will comply with applicable law, executive orders, DoD, IC, and NRO policies and procedures regarding information security, including with regard to access controls and monitoring.

c. Data Quality

NRO Components will maintain all personal information of non-U.S. persons collected through signals intelligence activities under the same data quality standards applied to equivalent personal information of U.S. persons and in accordance with the requirements outlined in Intelligence Community Directive 203, *Analytic Standards*.

d. Oversight

1. Office of General Counsel

SUBJECT: EXECUTIVE ORDER 14086 - ENHANCING SAFEGUARDS FOR UNITED STATES SIGNALS INTELLIGENCE ACTIVITIES

The NRO Office of General Counsel (OGC) shall review implementation of these policies and procedures annually.

All NRO personnel should report any potential instance of non-compliance with applicable policies and procedures to the OGC and Office of Policy and Strategy (OP&S). OGC and OP&S, in consultation with the NRO Office of Inspector General (OIG) and the NRO PCLPO, as appropriate, shall determine what, if any, corrective actions are necessary and appropriate. Should the NRO PCLP, in coordination with OGC, determine that an incident of non-compliance is a "significant incident of non-compliance" as defined in Section 4(l) of EO 14086, the determination will be reported immediately to the D/NRO, Secretary of Defense, and the DNI, who shall ensure that any necessary actions are taken to remediate it and prevent is recurrence.

2. Inspector General

Pursuant to NRO Directive, all NRO personnel are required to report to the NRO OIG any violation of law, regulation, executive order, or deficiency related to waste, fraud, and/or abuse involving NRO programs, operations, or personnel. NRO personnel may also report potential instances of noncompliance with U.S. law, these policies and procedures, or other matters of concern to the NRO OIG.

3. Assistance to the Civil Liberties Protection Officer

The NRO will provide the Civil Liberties Protection Officer (CLPO) from the Office of the Director of National Intelligence access to information necessary to conduct the reviews described in either Section 3(c)(i) or Section 3(d)(i) of EO 14086 and implemented by Intelligence Community Directive 126, consistent with the protection of intelligence sources and methods. NRO personnel shall not take any actions designed to impede or improperly influence CLPO's review of qualifying complaints or Data Protection Review Court's (DPRC) review of the CLPO's determination of such pursuant to the Signals Intelligence Redress Mechanism. NRO shall comply with any CLPO determination to undertake appropriate remediation, subject to any contrary determination of the DPRC, and, further, shall comply with any determination by a DPRC panel to undertake appropriate remediation.

4. Assistance to the Privacy and Civil Liberties Oversight Board

The NRO will provide the Civil Liberties Protection Officer (CLPO) from the Office of the Director of National Intelligence access to information necessary to conduct the annual review of the signals intelligence redress mechanism described in Section 3(e) of EO 14086, consistent with the protection of intelligence sources and methods.

SUBJECT: EXECUTIVE ORDER 14086 - ENHANCING SAFEGUARDS FOR UNITED STATES SIGNALS INTELLIGENCE ACTIVITIES

IV. Training

All NRO personnel who have access to information that is subject to these policies and procedures will receive introductory and annual training on applicable requirements. Successful completion of such training is a prerequisite to initial and continued access to the systems and records that contain information governed by EO 14086 and these policies and procedures. NRO will monitor completion of training requirements to ensure compliance with this provision.

V. Deviations from these Procedures

The NRO Director (DNRO) or Principal Deputy Director (PDDNRO), or designee, 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, an NRO component's director, or the senior NRO representative present may approve a departure from these procedures. The DNRO or PDDNRO, and the General Counsel, will be notified as soon thereafter as possible. The OGC will provide prompt written notice of any such departures to the Department of Defense Senior Intelligence Oversight Official, the Office of the Director of National Intelligence, and the National Security Division of the Department of Justice stating why advance approval was not possible and describing the actions taken to ensure activities were conducted lawfully. 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 NRO. Questions on the applicability or interpretation of these procedures should be directed to OGC and OP&S who, in consultation with the OIG, as appropriate, shall determine such applicability or interpretation.

C.J. Scolese
Director