NATIONAL RECONNAISSANCE OFFICE

14675 Lee Road Chantilly, VA 20151-1715

Office of the Director Policy Note

Number 2015-01

23 January 2015

PRESIDENTIAL POLICY DIRECTIVE 28 PROCEDURES

I. Introduction

Presidential Policy Directive 28 (PPD-28) regarding signals intelligence activities issued 17 January 2014, sets forth principles to guide why, whether, when, and how the United States (U.S.) conducts signals intelligence activities for authorized foreign intelligence and counterintelligence purposes. In particular, Section 4 of PPD-28 articulates principles for safeguarding personal information collected from signals intelligence activities and requires Intelligence Community (IC) elements to establish policies and procedures to apply these principles, in a manner consistent with technical capabilities and operational needs. This document constitutes the PPD-28 policies and procedures of the National Reconnaissance Office (NRO).

NRO is a joint Department of Defense (DoD) - IC organization responsible for developing, launching, and operating the United States' signals, imagery, and communications intelligence satellites. Data collected by NRO on behalf of the National Security Agency (NSA), National Geospatial-Intelligence Agency, and other NRO Mission Partners is used by these Mission Partners to produce intelligence products for the President, congress, national policy makers, warfighters, and civil users.

II. General Provisions and Authorities

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

Pursuant to Section 1.7(d) of Executive Order 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."

III. <u>Safeguarding Personal Information Collected through Signals</u> 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

¹ These procedures do not alter the rules applicable to U.S. persons found in the Foreign Intelligence Surveillance Act, Executive Order 12333, Bureau of Intelligence and Research's (INR) guidelines approved by the Attorney General pursuant to Sec. 2.3 of Executive Order 12333, or other applicable law.

SUBJECT: Presidential Policy Directive 28 Procedures

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. NRO also conducts research, development, test, and evaluation to enhance NSA's signals intelligence processing capabilities. In addition, NRO receives from other IC elements signals intelligence information that has been evaluated, minimized, or otherwise included in finished intelligence products subject to - among other requirements - the provisions of PPD-28.²

1. Dissemination³

NRO 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 Executive Order 12333. NRO 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, NRO will presume that any evaluated or minimized signals intelligence information it receives from other IC elements meets these standards. NRO will disseminate such information in accordance with applicable policies and procedures.

2. Retention

NRO 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 Section 2.3 of Executive Order 12333. NRO 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 it possesses specific information to the contrary, NRO will presume that any evaluated

² Such PPD-28 provisions include those in Section 1, such as (i) the U.S. 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 or 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 INR suspects that signals intelligence disseminated to it may have been collected or disseminated in a manner inconsistent with PPD-28, it shall so notify appropriate officials at the IC element that disseminated the signals intelligence.

³ Dissemination is the transmission, communication, sharing, or passing of information by any means, including oral, electronic, or physical means.

SUBJECT: Presidential Policy Directive 28 Procedures

or minimized signals intelligence information it receives from another IC element meets these standards. NRO will retain such information in accordance with applicable record retention policies.

b. Data Security and Access

Access to personal information of both U.S. and non-U.S. persons collected through signals intelligence activities - when identifiable - is restricted to those personnel who have a need to access that information in the performance of authorized duties in support of NRO's mission. 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 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

Personal information of both U.S. and non-U.S. persons collected through signals intelligence activities — when identifiable — shall be deleted as consistent with applicable NRO, DoD, and IC standards. Particular care should be taken to ensure only the technical characteristics of the data shall be retained as consistent with NRO's mission and applicable NRO, DoD, and IC standards.

d. Oversight

The NRO Signals Intelligence Compliance Officer (SCO) within NRO shall review implementation of these policies and procedures annually and report to the Office of General Counsel/Intelligence Oversight (OGC/IO), regarding the application of the safeguards contained herein and in Section 4 of PPD-28 more generally, as applicable.

Instances of non-compliance with these policies and procedures shall be reported to the NRO SCO and OGC/IO. NRO SCO and OGC/IO, in consultation with the Office of Inspector General (OIG), Office of the Deputy Chief Management Officer, and the Director of National Intelligence (DNI), as appropriate, shall determine what, if any, corrective actions are necessary and appropriate.

Significant instances of non-compliance with these policies and procedures involving the personal information of any person collected through signals intelligence activities shall be reported promptly to the NRO SCO and OGC/IO, who in turn will report them to the DNI pursuant to Section 4 of PPD-28.

SUBJECT: Presidential Policy Directive 28 Procedures

IV. Training

NRO 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.

V. Deviations from these Procedures

The NRO SCO 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 NRO SCO or the NRO SCO's senior representative present may approve a departure from these procedures. The Legal Adviser will be notified as soon thereafter as possible. The Legal Adviser will provide prompt written notice of any such departures to the Office of the Director of National Intelligence 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.

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 Office of Policy and Strategy/Signals Intelligence Compliance Group and OGC/IO who, in consultation with the OIG, as appropriate, shall determine such applicability or interpretation.

Director