Drug Enforcement Administration, Office of National Security Intelligence Presidential Policy Directive 28 – Policies and Procedures

I. Introduction

Presidential Policy Directive 28 regarding signals intelligence (SIGINT) activities (hereinafter "PPD-28"), issued January 17, 2014, articulates principles to guide why, whether, when, and how the United States conducts SIGINT activities for authorized foreign intelligence and counterintelligence purposes. Specifically, Section 4 of PPD-28 sets forth principles for safeguarding personal information collected from SIGINT activities and requires Intelligence Community (IC) elements to establish policies and procedures to apply such principles, consistent with technical capabilities and operational needs. This document constitutes the PPD-28 policies and procedures of the Drug Enforcement Administration (DEA), Office of National Security Intelligence (ONSI). ONSI, a component of DEA, 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 Executive Order 12333, as amended (EO 12333).

ONSI's primary mission is to facilitate full and appropriate intelligence coordination and information sharing with other members of the IC and homeland security elements to enhance our Nation's efforts to reduce the supply of drugs, protect our national security, and combat global terrorism.

II. General Provisions and Authorities

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

ONSI is not authorized to conduct – and does not conduct – SIGINT activities.

III. Safeguarding Personal Information Collected through SIGINT

The following policies and procedures apply to ONSI's safeguarding of personal information collected by the IC through SIGINT activities.[1]

(A) *Minimization*

ONSI does not have access to unevaluated, raw, or unminimized SIGINT, including SIGINT collected in bulk. ONSI does receive from other IC elements SIGINT

[1] These procedures do not alter the rules applicable to U.S. persons found in the Foreign Intelligence Surveillance Act, Executive Order 12333, or other applicable law.

information[2] that has been evaluated, minimized, or otherwise included in finished intelligence products subject to – among other requirements – the provisions of PPD-28.[3]

(i) Dissemination[4]

ONSI will disseminate personal information of non-U.S. persons collected through SIGINT activities only if dissemination of comparable information concerning U.S. persons would be permitted under Section 2.3 of EO 12333. ONSI 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, ONSI will presume that any evaluated or minimized SIGINT information it receives from other IC elements meets these standards. ONSI will disseminate such information in accordance with applicable ONSI, DEA and IC policies and procedures. Dissemination of personal information to a foreign government is permitted only if: the dissemination is consistent with the interests of the United States, including U.S. national security interests; the dissemination complies with any policy guidance, treaties, or agreements imposing further requirements on the dissemination or use of the information; and the dissemination complies with national and IC foreign disclosure release guidance.

(ii) Retention

ONSI will retain personal information of non-U.S. persons collected through SIGINT activities only if retention of comparable information concerning U.S. persons would be permitted under Section 2.3 of EO 12333. ONSI 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,

---

[2] The sources of or methods of obtaining specific information contained in evaluated or finished intelligence products may not in all cases be evident to ONSI 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 SIGINT 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) SIGINT 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) SIGINT activities shall be as tailored as feasible. If ONSI identifies signals intelligence disseminated to ONSI that it believes may have been collected in a manner that is not consistent with PPD-28, it shall notify appropriate officials at the IC element that collected the SIGINT.

[4] For purposes of these procedures, dissemination means the transmission, communication, sharing, or passing of information outside of DEA by any means, including oral, electronic, or physical means.

ONSI will presume that any evaluated or minimized SIGINT information it receives from another IC element meets these standards. ONSI will retain such information in accordance with applicable record retention policies.

(B) *Data Security and Access*

Access to personal information collected through SIGINT 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 ONSI or DEA 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 ONSI, DEA, and the IC.

Classified information will be stored appropriately in a secured, certified, and accredited facility or container, on approved information systems and databases, and in accordance with other applicable requirements. Electronic systems used by ONSI in which such information may be stored will comply with applicable law, Executive Orders, and IC and DEA 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 SIGINT activities – when identifiable – shall be included in ONSI intelligence products only as consistent with applicable IC standards set forth in relevant IC directives.

(D) *Oversight*

The Chief of ONSI and the Office of Chief Counsel shall review implementation of these policies and procedures annually and report to the DEA Deputy Chief of Intelligence regarding the application of the safeguards contained herein and in Section 4 of PPD-28 more generally, as applicable.

ONSI shall ensure that it makes available to its workforce information on how ONSI personnel may securely report violations of law, rule, or regulation. Instances of non-compliance with these policies and procedures shall be reported to the Chief of ONSI, who shall report them to the Deputy Chief of Intelligence. The Deputy Chief of Intelligence, in consultation with the Office of Chief Counsel and the Inspection Division, as appropriate, shall determine what, if any, corrective actions are necessary.

Significant instances of non-compliance involving the personal information of any person collected through SIGINT activities shall be reported promptly by the Chief of ONSI, who in turn will report them to the DNI pursuant to Section 4 of PPD-28.

IV. Training

ONSI personnel whose duties require access to personal information collected through SIGINT activities will receive annual training on the requirements of these policies and procedures. Successful completion of such training is a prerequisite to accessing such information.

V. Deviations from these Procedures

The Chief of ONSI 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 Chief of ONSI or his senior representative present may approve a departure from these procedures. The Chief of ONSI and the Office of Chief Counsel will be notified as soon thereafter as possible. After consultation with the Office of Chief Counsel, the Chief of ONSI 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 ONSI. Questions on the applicability or interpretation of these procedures should be directed to the Chief of ONSI, who shall determine such applicability or interpretation, in consultation with the Office of Chief Counsel, as appropriate.

Arthur A. Doty
Deputy Chief of Intelligence
Office of National Security Intelligence
Drug Enforcement Administration

11/5/15
Date