PPD-28 Section 4 Procedures

January 12, 2015

Presidential Policy Directive 28 (PPD-28) [1] articulates principles to guide United States SIGINT activities for authorized foreign intelligence and counterintelligence purposes. In response to PPD-28 Section 4, NSA has developed Supplemental Procedures to United States Signals Intelligence Directive, USSID SP0018.[2] USSID SP0018 implements the Attorney General-approved procedures contained in Department of Defense (DoD) Regulation 5240.1-R and its Classified Annex that govern NSA's SIGINT activities. USSID SP0018 prescribes specific minimization policies and procedures for U.S. Persons, and assigns responsibilities to assure that the missions and functions of the United States SIGINT System (USSS) are conducted in a manner that safeguards the constitutional rights of U.S. Persons. All personnel who are conducting E.O. 12333 SIGINT activities under the direction, authority, or control of the Director of the National Security Agency throughout the SIGINT lifecycle are responsible to protect the privacy of U.S. Persons.

PPD-28 Section 4 directs the Intelligence Community (IC) to establish policies and procedures for safeguarding personal information collected during signals intelligence activities. NSA's Supplemental Procedures are the guidance and procedures for implementing this direction from the President. Consistent with the requirements of Section 4.(a), NSA's Supplemental Procedures extend comparable safeguards currently provided for U.S. Persons to all persons, regardless of nationality. Section 4.(b) requires IC elements to issue procedures by 17 January 2015, one year after the President released PPD-28. As specified in section 4.(c), NSA worked with the White House in developing these policies and procedures to ensure the proper civil liberties and privacy safeguards are in place.

The new Supplemental Procedures are entitled "USSID SP0018 Supplemental Procedures for the Collection, Processing, Retention, and Dissemination of Signals Intelligence Information and Data Containing Personal Information of Non-United States Persons," and implement the privacy and civil liberties protections afforded to *non-U.S. persons* in a manner that is comparable, to the extent consistent with national security, to the privacy protections afforded to U.S. persons. These new Supplemental Procedures are written as a guide to SIGINT

---

[1] http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities Released by the White House on January 17, 2014, PPD-28 states that, "signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information."

[2] https://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf USSID SP0018 was approved for release by the National Security Agency on 13 November 2013.

professionals. Wherever possible, language in the Supplemental Procedures mirrors the terminology and structure of parallel provisions in USSID SP0018 and in PPD-28.

UNITED
STATES
SIGNALS
INTELLIGENCE
DIRECTIVE

(U) USSID SP0018: SUPPLEMENTAL PROCEDURES FOR THE COLLECTION, PROCESSING, RETENTION, AND DISSEMINATION OF SIGNALS INTELLIGENCE INFORMATION AND DATA CONTAINING PERSONAL INFORMATION OF NON-UNITED STATES PERSONS

ISSUE DATE:

(U) USSID SP0018 Supplemental Procedures for the Collection, Processing, Retention and Dissemination of Signals Intelligence Information and Data Containing Personal Information of Non-United States Persons establishes guidance and procedures for implementing Presidential Policy Directive (PPD) -28.

(U) This is the initial issuance of USSID SP0018 Supplemental Procedures for implementing PPD-28.

(U) OFFICE OF PRIMARY RESPONSIBILITY: NSA/CSS, Signals Intelligence Directorate, Signals Intelligence Policy and Corporate Issues Staff.

(U) The Executive Agent for this USSID is:

Ronald S. Moultrie

Ron Moultrie 12 JANUARY 2015
Signals Intelligence Director

(U) TABLE OF CONTENTS

(U) Letter of Promulgation

(U) Sections

SECTION 1	(U) Preface
SECTION 2	(U) References
SECTION 3	(U) Policy
SECTION 4	(U) Collection
SECTION 5	(U) Processing
SECTION 6	(U) Retention
SECTION 7	(U) Dissemination
SECTION 8	(U) Responsibilities

(U) Refer to the U.S. SIGINT System Dictionary for all signals intelligence (SIGINT) terms and definitions.

(U) USSID SP0018 SUPPLEMENTAL PROCEDURES FOR THE COLLECTION, PROCESSING, RETENTION, AND DISSEMINATION OF SIGNALS INTELLIGENCE INFORMATION AND DATA CONTAINING PERSONAL INFORMATION OF NON-UNITED STATES PERSONS

SECTION 1 - (U) PREFACE

(U) Purpose

1.1 (U) USSID SP0018 prescribes policies and procedures and assigns responsibilities to ensure that the missions and functions of the United States SIGINT System (USSS) are conducted in a manner that safeguards the constitutional rights of U.S. persons. These Supplemental Procedures implement the privacy and civil liberties protections afforded to non-U.S. persons, by Presidential Policy Directive No. 28 (PPD-28), "Signals Intelligence Activities," dated 17 January 2014.

(U) Scope

1.2 (U) Unless otherwise specified, these Supplemental Procedures shall apply to SIGINT activities conducted in order to acquire communications or information about communications, except that it shall not apply to SIGINT activities undertaken to test or develop SIGINT equipment or capabilities. The provisions of Annex D to USSID SP0018 govern SIGINT activities undertaken to test or develop SIGINT equipment or capabilities.

1.3 (U) For purposes of these Supplemental Procedures, the term "foreign intelligence" includes foreign intelligence and counterintelligence.

1.4 (U) Unless otherwise stated, these Supplemental Procedures use the same definitions contained in Section 9 of USSID SP0018.

(U) Departures

1.5 (U) Generally. If, due to unanticipated or extraordinary circumstances, NSA determines that it must take action in apparent departure from these procedures to protect the national security of the United States, such action may be taken upon the

approval of the NSA Director or a designee, following consultation with the Office of the Director of National Intelligence, the National Security Division of the Department of Justice, and the Office of the Secretary of Defense.

1.6 (U) Departures in Emergency Situations. If there is insufficient time for approval of a departure from these procedures in accordance with the preceding paragraph because of the immediacy or gravity of a threat to the safety of persons or property or to the national security, the NSA Director or the Director's senior representative present may approve a departure from these procedures. The General Counsel of NSA will be notified as soon thereafter as possible. The General Counsel of NSA will provide prompt written notice of any such departures to the Office of the Director of National Intelligence, to the National Security Division of the Department of Justice, and to the Office of the Secretary of Defense. 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.

1.7 (U) Nothing in these procedures shall prohibit or restrict:

a. (U) The retention, processing, analysis or dissemination of information necessary to avoid unauthorized collection, retention, or dissemination; or to avoid the collection, retention, and dissemination of information that is not foreign intelligence information;

b. (U) The retention of information for data integrity backup purposes, provided that only personnel responsible for maintaining and administering such information have access to it. In the event that information retained for backup purposes must be restored, NSA shall apply these procedures to the restored information. Information will be retained for data backup purposes for such time as is reasonably necessary;

c. (U) NSA's ability to conduct vulnerability or network assessments in order to ensure that NSA systems are not or have not been compromised. Notwithstanding any other section in these procedures, information used by NSA to conduct vulnerability or network assessments may be retained for one year solely for that limited purpose. Any information retained for this purpose may be disseminated only in accordance with the applicable provisions of these procedures;

d. (U) The retention, processing, analysis or dissemination of information necessary to perform lawful oversight functions, including lawful oversight functions of the Congress of the United States, the Department of Justice, Office of the Director of National Intelligence, or the applicable Offices of the Inspectors General;

e. (U) The retention, processing, analysis or dissemination of information necessary to comply with law; an order of a federal court or the rules of such a court; or these procedures.

SECTION 2 - (U) REFERENCES

2.1 (U) The following documents are references to these Supplemental Procedures:

a. (U) 50 U.S.C. 1801, et seq., Foreign Intelligence Surveillance Act (FISA) of 1978, as amended.

b. (U) Executive Order 12333, "United States Intelligence Activities," as amended 30 July 2008.

c. (U) Presidential Policy Directive No. 28, "Signals Intelligence Activities," dated 17 January 2014.

d. (U) Department of Defense Directive 5100.20, "National Security Agency/Central Security Service (NSA/CSS)," dated 26 January 2010.

SECTION 3 - (U) POLICY

(U) Policy and the USSS Foreign Communications Mission

3.1 (U) The collection of SIGINT shall be authorized by statute or Executive Order, proclamation, or other Presidential directive and undertaken in accordance with the Constitution and applicable statutes, Executive Orders, proclamations, and Presidential directives.

3.2 (U) Privacy and civil liberties shall be integral considerations in the planning of USSS SIGINT activities. The USSS shall not collect SIGINT for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, color, gender, sexual orientation, or religion.

3.3 (U) The policy of the USSS is to TARGET or COLLECT only FOREIGN COMMUNICATIONS for foreign intelligence purposes to support national and

departmental missions, including support for the conduct of military operations. If the USSS COLLECTS personal information of non-U.S. persons, it will process, analyze, disseminate, and retain such personal information only in accordance with these Supplemental Procedures. The USSS shall apply the term "personal information" in a manner that is consistent for U.S. persons and non-U.S. persons. Accordingly, for the purposes of these Supplemental Procedures, the term "personal information" shall cover the same types of information covered by "information concerning U.S. persons" under Section 2.3 of Executive Order 12333.

3.4 (U) The collection of foreign private commercial information or trade secrets is authorized only to protect the national security of the United States or its partners and allies. It is not an authorized foreign intelligence or counterintelligence purpose to collect such information to afford a competitive advantage to U.S. companies and U.S. business sectors commercially. Certain economic purposes, such as identifying trade or sanctions violations or government influence or direction, shall not constitute competitive advantage.

3.5 (U) SIGINT activities shall be as tailored as feasible. In determining whether to collect SIGINT, the USSS shall consider the availability of other information, including from diplomatic and public sources. Such appropriate and feasible alternatives to SIGINT should be prioritized.

SECTION 4 - (U) COLLECTION

4.1 (U) SIGINT activities that take place in response to foreign intelligence requirements, for example, those specified in the National Intelligence Priorities Framework, the National SIGINT Priorities Framework, and such follow-on direction or guidance that may be provided, as appropriate, by the President, the Director of National Intelligence, the Secretary of Defense, or DIRNSA/CHCSS as the SIGINT Functional Manager may result in the acquisition of communications that contain personal information of non-U.S. persons.

4.2 (U) Whenever practicable, collection will occur through the use of one or more SELECTION TERMS in order to focus the collection on specific foreign intelligence targets (e.g., a specific, known international terrorist or terrorist group) or specific foreign intelligence topics (e.g., the proliferation of weapons of mass destruction by a foreign power or its agents). In addition, if a collection method is regulated by FISA, the collection method will not be employed until the collection has been authorized

in the manner prescribed by FISA. Collection acquired as the result of an authorization under FISA will be handled in accordance with these procedures and with any applicable minimization procedures adopted by the Attorney General and approved by the Foreign Intelligence Surveillance Court to govern the collection. For collection that is not regulated by FISA, the collection will be handled in accordance with these procedures and USSID SP0018, including its Annexes, as applicable.

SECTION 5 - (U) PROCESSING

(U) Intercepted Material

5.1 (U) Forwarding of Intercepted Material. FOREIGN COMMUNICATIONS collected by the USSS may be forwarded as intercepted to NSA/CSS, intermediate processing facilities, and collaborating centers for further processing and analysis to determine whether the communications contain foreign intelligence.

5.2 (U) Information from nonpublic communications acquired in bulk[1] that contain personal information to, from, or about non-U.S. persons may be used only for the purposes of detecting and countering:[2]

a. (U) Espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests;

---

[1] (U) References to SIGINT collected in "bulk" mean the authorized collection of large quantities of SIGINT data that, because of technical or operational considerations, is acquired without the use of discriminants (e.g., without the use of specific identifiers or selection terms).

[2] (U) The limitations contained in this section do not apply to SIGINT data that is temporarily acquired to facilitate targeted collection, such as search and development activities permitted by Paragraph E1.2.a. of Annex E of USSID SP0018 or the processing of a signal that is necessary to select specific communications for forwarding for intelligence analysis. In contrast, intelligence analysis, such as communications metadata analysis, of SIGINT data collected in bulk that has not been limited through the use of one or more SELECTION TERMS (as described above in paragraph 4.2) will be subject to the limitations contained in this section.

b. (U) Threats to the United States and its interests from terrorism;

c. (U) Threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction;

d. (U) Cybersecurity threats;

e. (U) Threats to U.S. or allied armed forces or other U.S or allied personnel; and

f. (U) Transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes described above.

SECTION 6 - (U) RETENTION

(U) Retention of Communications

6.1 (U) Retention of Nonpublic Communications that Contain Personal Information of Non-U.S. Persons.

a. (U) Nonpublic communications that are acquired by the USSS that contain personal information of non-U.S. persons may be retained in their original or transcribed form only as follows: for up to 5 years unless the Director of National Intelligence (DNI) or the DNI's designee has expressly determined in writing that continued retention is in the national security interests of the United States. Information that has not been processed into an intelligible form because of unknown communication methods, encryption, or other methods of concealing secret meaning is not subject to the foregoing retention limit; however, the up-to-5-year retention period for such information will begin when the information has been made intelligible.

b. (U) Communications that could be disseminated under Section 7, below (i.e., without elimination of references to specific non-U.S. persons or deletion of personal information of non-U.S. persons) may be retained in their original or transcribed form.

c. (U) Personal information of non-U.S. persons obtained during SIGINT operations shall be processed and stored under conditions that

provide adequate protection and prevent access by unauthorized persons, consistent with the applicable safeguards for sensitive information contained in relevant Executive Orders, proclamations, Presidential Directives, Intelligence Community (IC) Directives, and associated policies. Access to such personal information of non-U.S. persons shall be limited to authorized personnel with a need to know the information to perform their mission, consistent with the personnel security requirements of relevant Executive Orders, IC Directives, and associated policies. Such personnel will be provided appropriate and adequate training concerning the requirements of these procedures.

SECTION 7 - (U) DISSEMINATION

(U) Focus of SIGINT Products and Services

7.1 (U) All SIGINT products and services will be written so as to focus solely on the provision of foreign intelligence to support national and departmental missions, including support for the conduct of military operations.

(U) Dissemination of Personal Information

7.2 (U) Personal information of non-U.S. persons obtained with the consent of the individual to whom it pertains may be disseminated in accordance with the terms of the consent. The USSS may also disseminate personal information, including personal information that specifically identifies or tends to identify one or more non-U.S. persons, if the personal information (i) is publicly available; (ii) is related to an authorized foreign intelligence requirement; (iii) is related to a crime that has been, is being, or is about to be committed; or (iv) indicates a possible threat to the safety of any person or organization. If the USSS is disseminating the personal information because it relates to a foreign intelligence requirement, it may not disseminate it solely because of the person's foreign status. Thus, for example, personal information about the routine activities of a non-U.S. person would not be disseminated without some indication that the personal information is related to an authorized foreign intelligence requirement.

(U) When disseminating unevaluated SIGINT that may contain personal information, the USSS should inform the recipient that the dissemination may contain personal

information so that the recipient can take appropriate steps to protect that information.

(U) Improper Dissemination

7.3 (U) If personal information of a non-U.S. person is improperly disseminated, the incident must be reported to the SIGINT Directorate's (SID's) Information Sharing Services Group (S1S) and Oversight and Compliance Organization (SV) within 24 hours upon recognition of the error for remediation and follow-on reporting to the DNI in accordance with the provisions of PPD-28.

SECTION 8 - (U) RESPONSIBILITIES

(U) Inspector General

8.1 (U) The NSA/CSS Inspector General (IG) may perform general oversight of NSA/CSS activities to ensure compliance with these Supplemental Procedures.

(U) General Counsel

8.2 (U) The NSA General Counsel (GC) shall provide legal advice and assistance to all elements of the USSS regarding the requirements of PPD-28 and the implementation guidance contained in these Supplemental Procedures.

(U) Civil Liberties and Privacy Director

8.3 (U) The NSA/CSS Civil Liberties and Privacy Director shall:

a. (U) Provide civil liberties and privacy advice and assistance regarding the requirements of PPD-28 and the implementation guidance contained in these Supplemental Procedures.

b. (U) Implement the guidance issued by the DNI for conducting SIGINT reviews and assessments from a civil liberties and privacy perspective, including assessments of the adequacy of safeguards to protect personal information that are either proposed or in place for new or unique SIGINT collection programs.

(U) Compliance Director

8.4 (U) The NSA/CSS Director of Compliance shall provide compliance advice and assistance regarding the requirements of PPD-28 and the implementation guidance contained in these procedures in coordination with SV.

(U) Enterprise Risk Management

8.5 (U) The NSA/CSS Enterprise Risk Management Officer shall provide advice and assistance regarding the requirements of PPD-28 and the implementation guidance contained in these procedures.

(U) Signals Intelligence Director

8.6 (U) The NSA/CSS Signals Intelligence Director shall:

a. (U) Ensure that all SIGINT production personnel conducting SIGINT production activities under DIRNSA/CHCSS authorities understand and maintain a high degree of awareness and sensitivity to the requirements of these Supplemental Procedures.

b. (U) Apply the provisions of these Supplemental Procedures to all SIGINT production activities governed by PPD-28 that are conducted under DIRNSA/CHCSS authorities. The SID staff focal point for USSID SP0018 matters is SV.

c. (U) Conduct necessary reviews of SIGINT production activities and practices governed by PPD-28 to ensure consistency with these Supplemental Procedures. These reviews will include periodic auditing against the standards required by these Supplemental Procedures.

d. (U) Ensure that all new major requirements levied on the USSS or internally generated activities are considered for review by the GC. All

activities that raise questions of law or the proper interpretation of these Supplemental Procedures must be reviewed by the GC prior to acceptance or execution.

(U) All Elements of the USSS

8.7 (U) All elements of the USSS shall:

a. (U) Implement these Supplemental Procedures upon receipt.

b. (U) Establish supplemental guidance, processes, and procedures or amend existing guidance, processes, and procedures as required to ensure adherence to these Supplemental Procedures. A copy of such shall be forwarded to NSA/CSS, Attn: SV.

c. (U) Immediately inform the SIGINT Director of any tasking or instructions that appear to require actions at variance with these Supplemental Procedures.

d. (U) In accordance with existing procedures, report to the NSA/CSS IG and consult with the NSA GC on all activities that may raise a question of compliance with these Supplemental Procedures. When a significant compliance issue occurs involving personal information of any person, regardless of nationality, collected as a result of SIGINT activities, the issue shall, in addition to any existing reporting requirements, be reported promptly to the Director, for follow-on reporting to the DNI in accordance with PPD-28.

Proceed To:
NSA | Director | SIGINT | SIGINT Staff | SIGINT Policy | USSID Index