U.S. Department of Homeland Security
United States Coast Guard

Commandant
United States Coast Guard

2703 Martin Luther King Avenue
STOP 7301
Washington, DC 20593-0001
Staff Symbol: CG-255
Phone: (202) 372-2733

COMDTINST 3820.5
23 JAN 2015

COMMANDANT INSTRUCTION 3820.5

Subj: COAST GUARD IMPLEMENTATION OF PRESIDENTIAL POLICY DIRECTIVE /PPD-28 – POLICIES AND PROCEDURES

Ref: (a) Presidential Policy Directive/PPD-28, Signals Intelligence Activities, The White House Office of the Press Secretary, January 17, 2014

1. PURPOSE. Shortly after the President issued Presidential Policy Directive 28 regarding signals intelligence activities (hereinafter "PPD-28"), the Office of the Director of National Intelligence (ODNI) established a multidisciplinary, interagency working group to discuss a common approach to developing additional appropriate safeguards that protect personal information, recognizing that every Intelligence Community (IC) element has different mission needs and requirements. The resulting policies and procedures reinforce the IC's commitment to protect the personal information of all people around the world, regardless of their nationality. This Commandant Instruction serves to acknowledge and reinforce this commitment within the Coast Guard Intelligence enterprise.

2. ACTION. All Coast Guard unit commanders, commanding officers, officers-in-charge, deputy/assistant commandants, and chiefs of headquarters staff elements shall comply with the provisions of this Instruction. Internet release is authorized.

3. DIRECTIVES AFFECTED. None.

4. DISCUSSION. PPD 28, issued January 17, 2014, articulates principles to guide why, whether, when, and how the United States conducts signals intelligence activities for authorized foreign intelligence and counterintelligence purposes. Specifically, Section 4 of PPD-28 sets forth principles for safeguarding personal information collected from signals intelligence 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 Coast Guard Intelligence, PPD-28 policies and procedures. Coast Guard Intelligence is comprised of personnel who engage in Law Enforcement Intelligence activity and National Intelligence activity. The Coast Guard National Intelligence Element (NIE) is the part of Coast Guard Intelligence that is also part 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.

DISTRIBUTION – SDL No. 165

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A																										
B	X	X																						X		
C																										
D																										
E																										
F																										
G																										
H																										

NON-STANDARD DISTRIBUTION:

a. *General Provisions and Authorities*. Pursuant to Section 1.7(h) of Executive Order 12333, as amended, the intelligence and counter intelligence elements of the Coast Guard are to "collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence including defense and defense-related information and intelligence to support national and departmental missions."

As a Service Cryptologic Component (SCC) and member of the United States SIGINT System (USSS), the Coast Guard Cryptologic Group (CGCG) is the only Coast Guard NIE authorized to conduct signals intelligence activities. Personnel assigned to the Coast Guard SCC conducts signals intelligence activities as tasked by the Director, NSA/Chief, CSS (DIRNSA/CHCSS), or the supported operational commander, when that operational commander has been delegated SIGINT Operational Tasking Authority (SOTA) from DIRNSA/CHCSS. These SIGINT activities, including the collection, processing, analysis, reporting, and dissemination of personal information, are governed by United States Signals Intelligence Directive (USSID) 18, the USSID 18 classified annex, as well as NSA's Supplemental procedures for the Collection, Retention, and Dissemination of Signals Intelligence Information and Data Containing Personal Information of Non-United States Persons.

b. *Safeguarding Personal Information Collected through Signals Intelligence*. In addition to the DoD and NSA/CSS policies applicable to Coast Guard NIE signals intelligence activities, the following policies and procedures apply to Coast Guard NIE safeguarding of personal information of non-U.S. persons collected through signals intelligence activities:[1]

(1) *Minimization* – Coast Guard NIE access to unevaluated, raw, or unminimized signals intelligence, including signals intelligence collected in bulk, is limited to those personnel assigned cryptologic responsibilities and subject to NSA/CSS policies. Coast Guard NIE does receive from other IC elements signals intelligence 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]

(a) Dissemination: For purposes of these policies and procedures, "dissemination" shall mean the transmission, communication, sharing or passing of information outside of Coast Guard by any means, including oral, electronic, or physical.

[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.

[2] The sources of or method of obtaining specific information contained in evaluated or finished intelligence products may not in all cases be evident to Coast Guard 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 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 Coast Guard 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 SIGINT.

1) Coast Guard NIE 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.

2) Coast Guard NIE 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.

3) Unless it possesses specific information to the contrary, Coast Guard NIE will presume that any evaluated or minimized signals intelligence information it received from other IC elements meets these standards.

4) Coast Guard NIE will disseminate such information in accordance with applicable Coast Guard and IC policies and procedures.

(b) Retention:

1) Coast Guard NIE 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.

2) Coast Guard NIE 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.

3) Unless it possesses specific information to the contrary, Coast Guard NIE will presume that any evaluated or minimized signals intelligence information it receives from other IC elements meets these standards.

4) Coast Guard NIE will retain such information in accordance with applicable record retention policies.

(2) *Data Security and Access* – Access to personal information collected through signals intelligence 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 Coast Guard or Departmental missions. Such information will be maintained in either electronic or physical form in secure facilities protected by appropriate 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 the Coast Guard, the Department, and the IC. Classified information will be stored appropriately in a secured, certified, and accredited facility, in secured databases and containers, and in accordance with other applicable requirements. Coast Guard's electronic system in which such information may be stored 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.

(3) *Data Quality* – Personal information of both U.S. and non-U.S. persons collected through signals intelligence activities – when identifiable – shall be included in Cost Guard intelligence products only as consistent with applicable IC standards of analytic tradecraft as set forth in relevant IC directives. In such instances, particular care should be taken to apply standards relating to the relevance and reliability of the information, consideration of alternative sources of information and interpretations of data, and objectivity in performing analysis.

(4) *Oversight* – The Office of Information and Intelligence Law within Coast Guard Headquarters shall review implementation of these policies and procedures annually and report to The Judge Advocate General 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 Chief, Office of Information and Intelligence Law, who shall report them to The Judge Advocate General and the Assistant Commandant for Intelligence. The Assistant Commandant for Intelligence, in consultation with The Judge Advocate General and Office of the Inspector General, as appropriate, shall determine what, if any, corrective actions are necessary. 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 Director of National Intelligence (DNI) pursuant to Section 4 of PPD-28.

c. *Training*. Coast Guard 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.

d. *Deviations from these Procedures*. The Assistant Commandant for Intelligence and Criminal Investigations (CG-2) must approve in advance any departures from these procedures, after consultation with the DNI and the National Security Division of the Department of Justice (DOJ). 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 immediacy or gravity of a threat to the safety of persons or property or to the national security, the Assistant Commandant (CG-2) or senior representative present may approve a departure from these procedures. The Assistant Commandant (CG-2) and The Judge Advocate General will be notified as soon thereafter as possible. Coast Guard NIE will provide prompt written notice of any such departure to the DNI and the National Security Division of the Department of Justice (DOJ). 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.

e. *Conclusion*. These procedures are set forth solely for internal guidance within the Coast Guard. Questions on the applicability or interpretation of these procedures should be directed to the Office of Intelligence Planning and Policy (CG-25), who shall determine such applicability or interpretation, in consultation with the Office of Information and Intelligence Law.

5. DISCLAIMER. This guidance is intended to provide operational guidance for Coast Guard personnel and is not intended to nor does it impose legally-binding requirements on any party outside the Coast Guard.

6. MAJOR CHANGES. None.

7. IMPACT ASSESSMENT. This directive reinforces current practices, establishes new principles that govern how we conduct SIGINT collection, and strengthens how we provide executive branch oversight of our SIGINT activities of which Coast Guard Intelligence personnel should be cognizant; there are no changes that are assessed to significantly impact the workload for Coast Guard Intelligence personnel or operational commands.

8. ENVIRONMENT ASPECT AND IMPACT CONSIDERATIONS. The development of this directive and the general policies contained within it have been thoroughly reviewed by the originating office and are found to be categorically excluded from further environmental analysis, in accordance with the National Environmental Policy Act Implementing Procedures and Policy for Considering Environmental Impacts, COMDTINST M16475.1 (series), Figure 2-1, (33). This directive will not have any of the following: significant cumulative impacts on the human environment; substantial controversy or substantial change to existing environmental conditions; or inconsistencies with any Federal, State, or local laws or administrative determinations relating to the environment. A written Categorical Exclusion Determination (CED) is not required.

9. DISTRIBUTION. No paper distribution will be made of this directive. An electronic version will be located on CG Portal:

   https://cgportal2.uscg.mil/library/directives/SitePages/Home.aspx.

10. RECORDS MANAGEMENT CONSIDERATIONS. This Manual has been thoroughly reviewed during the directives clearance process, and it has been determined there are further records scheduling requirements, in accordance with Federal Records Act, 44 U.S.C. 3101 et seq., NARA requirements, and Information and Life Cycle Management Manual, COMDTINST M5212.12 (series). This policy creates minor change to existing records management requirements."

11. FORMS/REPORTS. None.

12. REQUEST FOR CHANGES. All changes to this Manual will be coordinated by Commandant (CG-255).

C.J. Tomney, RADM /s/
U.S. Coast Guard
Assistant Commandant for Intelligence and
Criminal Investigations