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

Commandant
United States Coast Guard

2703 Martin Luther King Jr. Ave. SE
Washington, DC 20593-7318
Staff Symbol: CG-2
Phone: (202) 372-2700
Email: Rebecca.E.Ore@uscg.mil

3820
29 Jun 2023

MEMORANDUM

From: Rebecca E. Ore, RDML
CG COMDT (CG-2)

Reply to CG-LII
Attn of: Dorothy J. Hernaez, CAPT
Phone: (202) 372-2716

To: Coast Guard Intelligence Enterprise

Subj: PROCEDURES IMPLEMENTING ENHANCED SAFEGUARDS FOR SIGNALS INTELLIGENCE ACTIVITIES UNDER EXECUTIVE ORDER 14086

Ref: (a) Executive Order 14086, Enhancing Safeguards for United States Signals Intelligence Activities, October 14, 2022
(b) COMDTINST 3820.5, Coast Guard Implementation of Presidential Policy Directive/PPD-28 – Policies and Procedures, January 23, 2015

1. Ref. (a) bolsters the rigorous array of privacy and civil liberties safeguards that apply to United States signals intelligence activities, in recognition that such activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or where they may reside, and that all persons have a legitimate privacy interest in the handling of their personal information.

2. Ref. (a) directs the heads of the Intelligence Community (IC) elements to develop procedures that establish enhanced safeguards for personal information derived from signals intelligence activities.

3. This policy memorandum and its enclosed procedures establish the Coast Guard Intelligence Enterprise's implementing procedures under Ref. (a). This policy memorandum supersedes Ref. (b).

4. I direct the Coast Guard Intelligence Enterprise to immediately comply with the enclosed procedures. I further direct COMDT (CG-25) to immediately develop a Commandant Instruction that cancels Ref. (b) and implements the enclosed procedures.

#

Encl: (1) Procedures Implementing Enhanced Safeguards for Signals Intelligence Activities Under Executive Order 14086

ENCLOSURE 1

Coast Guard Procedures Implementing Enhanced Safeguards for Signals Intelligence Activities Under Executive Order 14086

1. BACKGROUND

a. Coast Guard National Intelligence Element.

(1) The national intelligence and counterintelligence elements of Coast Guard Intelligence (CG-2) comprise the Coast Guard national intelligence element (NIE), which is an element of the IC.

(2) Pursuant to Section 1.7(h) of E.O. 12333, the Coast Guard NIE is authorized 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."

(3) The cryptologic elements of the Coast Guard NIE are thus authorized to collect signals intelligence under the direction of Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS).

b. Coast Guard Signals Intelligence Activities.

(1) DIRNSA/CHCSS exercises operational control (OPCON) over all U.S. signals intelligence (SIGINT) activities, including activities performed by Coast Guard units.

(2) The Coast Guard Cryptologic Enterprise[1] (CGCE) is a Service Cryptologic Component (SCC) and element of the United States SIGINT System (USSS). As the designated Coast Guard signals intelligence units, CGCE is the only Coast Guard intelligence unit authorized to conduct signals intelligence activities.

(3) Personnel assigned to CGCE conduct signals intelligence activities as tasked by the DIRNSA/CHCSS, or the supported operational commander, when that operational commander has been delegated SIGINT Operational Tasking Authority (SOTA) from DIRNSA/CHCSS.

(4) CGCE follows authoritative guidance on all SIGINT activities from DIRNSA/CHCSS, especially pertaining to tasking, collection, processing, dissemination, standards, and training. As such, the Coast Guard's SIGINT activities are governed by United States Signals Intelligence Directive 18, its classified annex, as well as NSA's supplemental procedures (Ref. (c)).

[1] The Coast Guard Cryptologic Enterprise (CGCE) consists of the designated Coast Guard signals intelligence units. These include the Coast Guard Cryptologic Group, the Coast Guard Cryptologic Office, and all Coast Guard cryptologic detached units.

(5) The rest of the Coast Guard NIE does not conduct signals intelligence activities but may receive evaluated or minimized SIGINT reports from the CGCE.

2. PROCEDURES. The following safeguards fulfill the principles contained in subsections 2(a)(ii)-(iii) of Ref. (a).

a. Enhanced Safeguards Generally. The Coast Guard will use the following enhanced safeguards for signals intelligence activities,[2] as described under Ref. (a):

(1) Requiring signals intelligence activities to meet enumerated legitimate objectives;[3]

(2) Explicitly barring prohibited activities; and

(3) Requiring that signals intelligence activities be conducted only following a determination, based on a reasonable assessment of all relevant factors, that the activities are necessary to advance a validated intelligence priority and only to the extent and in a manner that is proportionate to the validated intelligence priority for which they have been authorized.

---

[2] References to signals intelligence and signals intelligence activities in this document also apply to information under Section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended. These procedures do not alter the rules applicable to U.S. persons found in the Foreign Intelligence Surveillance Act or orders issued pursuant to the Act, Executive Order 12333, guidelines approved by the Attorney General pursuant to Section 2.3 of Executive Order 12333, or other applicable law.

[3] "Enumerated legitimate objectives" include one or more of the following: (1) understanding or assessing the capabilities, intentions, or activities of a foreign government, a foreign military, a faction of a foreign nation, a foreign-based political organization, or an entity acting on behalf of or controlled by any such foreign government, military, faction, or political organization, in order to protect the national security of the United States and of its allies and partners; (2) understanding or assessing the capabilities, intentions, or activities of foreign organizations, including international terrorist organizations, that pose a current or potential threat to the national security of the United States or of its allies or partners; (3) understanding or assessing transnational threats that impact global security, including climate and other ecological change, public health risks, humanitarian threats, political instability, and geographic rivalry; (4) protecting against foreign military capabilities and activities; (5) protecting against terrorism, the taking of hostages, and the holding of individuals captive (including the identification, location, and rescue of hostages and captives) conducted by or on behalf of a foreign government, foreign organization, or foreign person; (6) protecting against espionage, sabotage, assassination, or other intelligence activities conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person; (7) protecting against threats from the development, possession, or proliferation of weapons of mass destruction or related technologies and threats conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person; (8) protecting against cybersecurity threats created or exploited by, or malicious cyber activities conducted by or on behalf of, a foreign government, foreign organization, or foreign person; (9) protecting against threats to the personnel of the United States or of its allies or partners; (10) protecting against transnational criminal threats, including illicit finance and sanctions evasion related to one or more of the other objectives identified in subsection (b)(i) of this section; (11) protecting the integrity of elections and political processes, government property, and United States infrastructure (both physical and electronic) from activities conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person; and (12) advancing collection or operational capabilities or activities in order to further a legitimate objective identified in subsection (b)(i) of this section (Ref. (a)).

b. Safeguarding Personal Information Collected[4] through Signals Intelligence: Coast Guard Cryptologic Enterprise (CGCE).

(1) Ref. (c) provides the entire USSS with procedures implementing Ref. (a) that govern the safeguarding of personal information of non-United States persons, including collection, minimization, dissemination, retention, data security and access, data quality, oversight and compliance, and reporting requirements.

(2) As an element of the USSS, the CGCE shall implement Ref. (a), Sections 2(c)(i)-(ii) and 2(c)(iii)(D), by following the procedures enumerated in Ref. (c), and all other applicable regulations and policies as directed by DIRNSA/CHCSS.

(3) In addition to following the procedures in Ref. (c), CGCE personnel shall follow the reporting, redress, and training requirements identified in sections 6.c., 6.d., and 6.e. below.

c. Safeguarding Personal Information Collected[5] through Signals Intelligence: Rest of Coast Guard NIE. The rest of the Coast Guard NIE (not within the USSS) may receive evaluated or minimized SIGINT from the CGCE or other IC partners. The rest of the Coast Guard NIE shall implement Ref. (a) in accordance with the following procedures to safeguard the information of non-US persons collected through signals intelligence activities.[6]

(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 to CGCE under the guidance and direction of DIRNSA.[7] However, the Coast Guard NIE does receive from other IC elements signals intelligence information that has been minimized, evaluated, or otherwise included in finished intelligence products subject to, among other requirements, the provisions of Ref. (a).

(a) Dissemination —

(i) For purposes of these procedures, "dissemination" shall mean the transmission, communication, sharing, showing, or passing of signals intelligence information outside of the Coast Guard NIE by any means, including oral, electronic, or physical means or by providing another entity with access to a Coast Guard NIE information system. The Coast Guard NIE shall disseminate personal information collected through signals intelligence

[4] The term "collection" as used in these procedures is defined in Ref. (h).

[5] The term "collection" as used in these procedures is defined in Ref. (h).

[6] The sources and methods used to collect specific information contained in evaluated or finished intelligence products may not be evident to the Coast Guard as a recipient of such intelligence products.

[7] Personnel assigned to CGCE will follow the controls and oversight mechanisms in Ref. (e) and any other guidance and direction provided by DIRNSA on signals intelligence activities, including bulk collections.

only in accordance with, and never to circumvent, applicable U.S. law, Presidential directives, IC directives, and policies and procedures.

(ii) The Coast Guard NIE shall 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 E.O. 12333.

(iii) The Coast Guard NIE shall take due account of the purpose of the dissemination, the nature and extent of the personal information being disseminated, and the potential for harmful impact on the person or persons concerned before disseminating personal information collected through signals intelligence to recipients outside the U.S. Government, including to a foreign government or international organization.

(iv) If the Coast Guard NIE is disseminating personal information of a non-U.S. person on the basis that it is foreign intelligence, the information must relate to an authorized intelligence requirement, and cannot be disseminated solely because of nationality or country of residence. Unless the Coast Guard NIE possesses specific information to the contrary, it shall presume that any evaluated or minimized signals intelligence information they receive from other IC elements that have adopted procedures implementing Ref. (a) meets this standard.

(v) The Coast Guard NIE shall disseminate within the U.S. Government such 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.

(vi) Dissemination of signals intelligence information must comply with Procedures 4 and 5 of Ref. (h) and other applicable Coast Guard implementing policy. In the event of a conflict between Ref. (h) (or other applicable Coast Guard policy) and these procedures pertaining to the dissemination of signals intelligence information, these procedures shall control.

(b) Retention —

(i) 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. Coast Guard NIE shall 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 applicable law, executive orders, including section 2.3 of E.O. 12333, agreements, and policies and

procedures, and shall subject such information to the same retention periods that would apply to comparable information concerning U.S. persons.

(ii) If the Coast Guard NIE is retaining personal information of a non-U.S. person on the basis that it is foreign intelligence, the information must relate to an authorized intelligence requirement, and cannot be retained solely because of non-U.S. person status. Coast Guard NIE personnel shall presume, unless they possess specific information to the contrary, that any evaluated or minimized signals intelligence information they receive from other IC elements that have adopted procedures implementing Ref. (a) meets these standards.

(iii) Coast Guard NIE shall delete non-U.S. persons' personal information that may no longer be retained in the same manner that comparable information concerning U.S. persons would be deleted.

(iv) Retention of signals intelligence information must comply with Procedures 3 and 5 of Ref. (h) and other applicable Coast Guard implementing policy. In the event of a conflict between Ref. (h) (or other applicable Coast Guard policy) and these procedures pertaining to the retention of signals intelligence information, these procedures shall control.

(2) Data Security and Access.

(a) Coast Guard NIE 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.

(b) Access to personal information collected through signals intelligence activities is restricted to those personnel who have a need to access that information in the performance of authorized duties in support of Coast Guard missions and have completed all required training as described under subsection 2(c)(iii)(B)(2) of Ref. (a). Such information, in either electronic or physical form, will be maintained in secure facilities protected by physical and technical safeguards, and with security measures designed to properly limit access to it. Such information will be safeguarded in accordance with applicable laws, executive orders, agreements, and policies and procedures.

(c) Classified information collected through signals intelligence activities will be stored appropriately in secured, certified, and accredited facilities, in secured databases and containers, and in accordance with other applicable requirements. Coast Guard electronic systems in which such information may be stored will comply with applicable law, executive orders, agreements, and policies and procedures regarding information security, including with regard to access controls and monitoring.

(d) CG-26, as the Coast Guard Deputy Chief Information Officer for Intelligence, in consultation with TJAG and CG-LII, will ensure that the electronic systems in which signals intelligence information is stored are certified under and adhere to established standards. Where signals intelligence information is stored on USSS information systems, Ref. (e) governs.

(3) Data Quality.

(a) Coast Guard NIE will maintain all personal information of non-U.S. persons collected through signals intelligence activities under the same data quality standard applied to equivalent personal information of U.S. persons.

(b) Personal information collected through signals intelligence activities — where such information can be so identified — shall be included in Coast Guard NIE intelligence products only as consistent with applicable IC standards of analytic tradecraft as set forth in relevant directives, including IC Directive 203, Analytic Standards. 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. Personal information should be included in intelligence products only when necessary to understand the product.

(4) Oversight.

(a) Coast Guard intelligence oversight officers (IOOs) within the Office of Information and Intelligence Law (CG-LII) shall audit and review implementation of these policies and procedures in accordance with intelligence oversight requirements specified in Ref. (i), and report to The Judge Advocate General (TJAG) (in TJAG's role as senior intelligence oversight official for the Coast Guard) regarding the application of the safeguards contained herein and in Ref. (a), as applicable, and to the Department of Homeland Security Office of General Counsel, in accordance with Ref. (i).

(b) The Coast Guard shall provide the ODNI CLPO and the Privacy and Civil Liberties Oversight Board with access to information necessary to conduct the annual review of the redress process described in Ref. (a), consistent with the protection of intelligence sources and methods.

(c) Coast Guard oversight, legal, and compliance officials have sufficient authority to conduct oversight and ensure compliance with the law and receive all information necessary to conduct their functions. No actions should be designed to impede or improperly influence their responsibilities.

(5) Reporting Non-Compliance.

(a) All Coast Guard NIE personnel should report instances of non-compliance with these policies and procedures to CG-LII. CG-LII, in consultation with TJAG (in his or her role as senior intelligence oversight official), shall promptly report instances of non-compliance to relevant entities to ensure their remediation in accordance with Ref. (i).

(b) In the event of a significant incident of non-compliance[8] as determined by CG-LII in consultation with TJAG, CG-LII shall promptly report such incident to the Assistant Commandant for Intelligence (CG-2), the Commandant of the Coast Guard (CCG), the Secretary of the Department of Homeland Security (S1), and the Director of National Intelligence (DNI), and conduct any additional reporting required under Ref. (i). Upon receipt of such report, CG-2, CCG, and the DNI shall ensure that any necessary actions are taken to remediate and prevent the recurrence of the significant incident of non-compliance.

(6) Inspector General. Consistent with Ref. (g), CGCE and Coast Guard NIE personnel are required to report criminal activity, including fraud, waste, and abuse involving Coast Guard activities, operations, programs, or personnel to the Office of the Inspector General of the Intelligence Community (IC IG) or to the DHS Office of the Inspector General (DHS OIG). Such personnel may also report other potential instances of non-compliance with U.S. law, these policies and procedures, or other matters of concern to the IC IG or DHS OIG.

d. Redress Mechanism.

(1) Individuals in "qualifying states" may seek redress via the independent and binding mechanism described in Refs. (a) and (f) through the submission of a "qualifying complaint" alleging a "covered violation" has occurred pertaining to personal information they reasonably believe to have been transmitted to the United States.[9]

(2) Coast Guard personnel shall provide all necessary assistance to the organizations providing the redress mechanism described in Refs. (a) & (f), including by providing the Office of the Director of National Intelligence Civil Liberties and Privacy Office (ODNI CLPO) with access to information necessary to conduct the reviews described in either Section 3(c)(i) or Section 3(d)(i) of Ref. (a), consistent with the protection of intelligence sources and methods. Coast Guard personnel shall not take any actions designed to impede or improperly influence the ODNI CLPO's review of qualifying complaints, or the Data Protection Review Court (DPRC) review of the CLPO's determination of such pursuant to the Signals Intelligence Redress Mechanism. The Coast Guard shall comply with any determination by the ODNI CLPO to undertake

[8] "Significant incident of non-compliance" means "a systemic or intentional failure to comply with a principle, policy, or procedure of applicable United States law that could impugn the reputation or integrity of an element of the Intelligence Community or otherwise call into question the propriety of an Intelligence Community activity, including in light of any significant impact on the privacy and civil liberties interests of the person or persons concerned" (Sec. 4(l) of Ref. (a)).

[9] "Qualifying states," "qualifying complaint," and "covered violation" are defined in Ref. (a).

appropriate remediation, subject to any contrary determination by the DPRC, and, further, shall comply with any determination by a DPRC panel to undertake appropriate remediation. ODNI CLPO and DPRC determinations are binding.

e. Training. All Coast Guard 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, and completion of training requirements will be monitored to ensure compliance with this provision.

f. Deviation from these Procedures. CG-2 must approve in advance any departures from these procedures, after consultation with the ODNI 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, a departure from these procedures may be approved in consultation with Chief, CG-LII. CG-2 and TJAG will be notified of any such departures as soon thereafter as possible. CG-2 will provide prompt written notice of any such departures stating why advance approval was not possible and describing the actions taken to ensure activities were conducted lawfully to the ODNI 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.

g. Internal Guidance and Interpretation. 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 CG-LII.

References

(a) Executive Order 14086, Enhancing Safeguards for United States Signals Intelligence Activities, October 14, 2022
(b) Presidential Policy Directive 28, Signals Intelligence Activities, January 17, 2014 (partially revoked pursuant to National Security Memorandum 14)
(c) Intelligence Community Directive 126, Implementation Procedures for the Signals Intelligence Redress Mechanism Under Executive Order 14086, December 6, 2022
(d) Intelligence Community Directive 120, Intelligence Community Whistleblower Protection, April 29, 2016
(e) NSA/CSS Policy 12-3 Annex C, Supplemental Procedures for the Collection, Processing, Querying, Retention, and Dissemination of Signals Intelligence Information and Data Containing Personal Information of Non-United States Persons (Draft)
(f) COMDTINST 3820.5, Coast Guard Implementation of Presidential Policy Directive/PPD-28 – Policies and Procedures, January 23, 2015
(g) COMDTINST M3820.12A, Coast Guard National Intelligence Activities Instruction Manual, January 2021
(h) COMDTINST M3821.14A, Coast Guard Intelligence Oversight Manual, April 2021
(i) Information Memorandum, Delegation of Signals Intelligence Operational Tasking Authority Over U.S. Coast Guard Tactical Signals Intelligence Units and Operations, April 18, 2012