U.S. Department of Homeland Security

United States Coast Guard

Coast Guard National Intelligence Activities Instruction Manual

COMDTINST M3820.12A
January 2021

THIS PAGE INTENTIONALLY LEFT BLANK

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

Commandant
United States Coast Guard

U.S. Coast Guard STOP 7301
2703 Martin Luther King Avenue, SE
Washington, DC 20593-7301
Staff Symbol: COMDT (CG-25)
Phone: (202) 372-2767
Fax: (202) 372-2973

COMDTINST M3820.12A
26 JAN 2021

COMMANDANT INSTRUCTION M3820.12A

Subj: COAST GUARD NATIONAL INTELLIGENCE ACTIVITIES.

Ref: (a) Executive Order 12333, United States Intelligence Activities (As Amended)

1. PURPOSE. This Manual establishes the mission of the Coast Guard National Intelligence Element (NIE) and sets forth policies and procedures for the conduct of intelligence activities by the Coast Guard NIE and oversight of those activities in a manner consistent with the protection of the constitutional rights of U.S. Persons and all others entitled to such protections.
2. ACTION. All Coast Guard unit commanders, commanding officers, officers-in-charge, deputy/assistant commandants, and chiefs of headquarters staff elements must ensure compliance with the provisions of this Manual. Internet release is authorized.
3. DIRECTIVES AFFECTED. This Manual supersedes COMDTINST M3820.12 "Coast Guard Intelligence Activities," dated 28 Aug 2003. This Manual cancels COMDTINST S3821.12, "Classified Supplement to Coast Guard Intelligence Activities", dated 28 Aug 2003.
4. DISCUSSION.
   a. Coast Guard Intelligence (CGI). Coast Guard Intelligence (CGI) is organized into two elements: the Law Enforcement Intelligence Element (LEIE) and the National Intelligence Element (NIE). In accordance with applicable law, the NIE conducts FI and CI activities as authorized by E.O. 12333, as amended, and the National Security Act of 1947, as amended, which designate the FI and CI elements of the Coast Guard as an Intelligence Community (IC) member. The LEIE conducts law enforcement intelligence activities as authorized by Coast Guard law enforcement and regulatory authorities. This Manual governs the conduct of FI and CI activities conducted by the NIE. This Manual does not pertain to LEIE activities.
   b. Coast Guard National Intelligence Element (NIE). The National Security Act of 1947, as

DISTRIBUTION – SDL No. 170

	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																						X				
B	X	X		X		X					X	X			X						X			X		
C	X	X								X												X		X		
D											X															
E																X		X				X				
F																										
G																										
H						X				X																

NON-STANDARD DISTRIBUTION:

amended (50 USC § 401a) establishes the national intelligence element of the Coast Guard as part of the IC. The term "national intelligence element" or "NIE" of the Coast excludes the LEIE.

c. IC Responsibilities. Consistent with E.O. 12333, as amended, the NIE, under the leadership of the Director of National Intelligence (DNI), and in cooperation with other IC elements, shall:

i. Collect and provide information needed by the President and, in the performance of executive functions, the Vice President, the National Security Council (NSC), the Homeland Security Council (HSC), the Chairman of the Joint Chiefs of Staff, senior military commanders, the Secretary of the Department of Homeland Security (DHS), and other executive branch officials and, as appropriate, the Congress of the United States;

ii. In accordance with priorities set by the President, collect information concerning, and conduct activities to protect against, international terrorism, proliferation of weapons of mass destruction, intelligence activities directed against the United States, international criminal drug activities, and other hostile activities directed against the United States by foreign powers, organizations, persons, and their agents;

iii. Analyze, produce, and disseminate intelligence;

iv. Conduct administrative, technical, and other support activities within the United States and abroad necessary for the performance of authorized activities, to include providing services of common concern for the IC as designated by the DNI in accordance with E.O. 12333;

v. Conduct research, development, and procurement of technical systems and devices relating to authorized functions and missions or the provision of services of common concern for the IC;

vi. Protect the security of intelligence related activities, information, installations, property, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the IC elements as are necessary;

vii. Take into account State, Local, Tribal and Territorial governments' and, as appropriate, private sector entities' information needs relating to national and homeland security;

viii. De-conflict, coordinate, and integrate all intelligence activities and other information gathering in accordance with § 1.3(b)(20) of E.O. 12333; and

ix. Perform such other functions and duties related to intelligence activities as the President may direct.

d. Coast Guard FI and CI Responsibilities. As directed by E.O. 12333 § 1.7(h), the NIE shall serve the information and intelligence needs of the Commandant of the Coast Guard, Secretary of DHS, and operate as an integrated part of the IC. Specifically, the Coast Guard NIE shall:

i. Collect (including through clandestine means), analyze, produce, and disseminate FI and CI, including defense and defense-related information and intelligence to support national and departmental missions;

ii. Conduct counterintelligence activities;

iii. Monitor the development, procurement, and management of tactical intelligence systems and equipment and conduct related research, development, and test and evaluation activities; and

iv. Conduct FI liaison relationships and intelligence exchange programs with foreign intelligence services, security services, or international organizations in accordance with E.O. 12333 § 1.3(b)(4), § 1.7(a)(6), and when operating as part of the Department of Defense, § 1.10(i) of E.O. 12333.

e. Individual Responsibilities. CGI component heads may issue implementing instructions for the conduct of authorized missions or functions consistent with the procedures in this issuance. In developing such instructions, CGI component heads must consult with Commandant (LII), Office of Privacy Management (CG-6P), and civil liberties officials.

i. Assistant Commandant for Intelligence (CG-2). As provided in Executive Order 13286 § 87, Commandant (CG-2), together with the Commandant of the Coast Guard (Commandant), are each considered a "Senior Official of the Intelligence Community," a term now referred to as the Head of the IC Element (HICE). Their duties and responsibilities are set forth in E.O. 12333.

ii. Commanders, Commanding Officers, and Directors of National Intelligence Element units, or units containing NIE personnel. Commanders, Commanding Officers, and Directors of National Intelligence Element units, or units containing NIE personnel will ensure that the NIE under their command comply with this Manual, and all applicable laws, executive orders, presidential directives, Intelligence Community directives, and other applicable directives that might govern the NIE.

iii. The Coast Guard Judge Advocate General (TJAG). TJAG is the Coast Guard NIE Senior Intelligence Oversight Official (SIOO) and is responsible for providing intelligence oversight for Coast Guard FI and CI activities. Consistent with E.O. 13462, as amended, TJAG must report intelligence oversight matters to the President's Intelligence Oversight Board through the DHS General Counsel. Chief, Office of Information and Intelligence Law (CG-LII) executes TJAG's SIOO duties.

f. Inspector General. Nothing in this Manual must interfere with the authority of the DHS Inspector General to carry out criminal investigations of civilian employees, investigations, or audits of Coast Guard activities.

g. Procedures. E.O. 12333, Part 2, requires the Coast Guard HICE to issue procedures on the conduct of intelligence activities taking place in the United States or directed against U.S. Persons. This Manual includes procedures that were developed in consultation with the DNI, with the approval of the Attorney General. All delegations of approval allowed by this Manual must be conveyed in writing. No approval authority may be delegated absent a written delegation.

h. EXECUTIVE ORDER. In accordance with Executive Order (E.O.) 12333, "United States Intelligence Activities," dated 4 December 1981, as amended in 2008, the Manual:

i. Recognizes that Coast Guard NIE personnel are authorized to conduct authorized foreign intelligence (FI) and counterintelligence (CI) activities effectively and in a manner that protects the privacy, civil liberties, and constitutional rights of the U.S. persons

ii. Prescribes procedures on the professional and lawful conduct of FI and CI activities carried out by NIE components, including the requirement to report violations of intelligence law, policy, or regulation that occur during FI or CI activities, as well as any other improper collection, retention, or dissemination of FI, CI, and U.S. persons information (USPI).

iii. Requires that Coast Guard FI and CI activities are carried out in compliance with applicable laws, executive orders, policies, and regulations that control such activities.

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. This update is a comprehensive rewrite to comply with the 2008 amendments to E.O. 12333. These guidelines substantially align with the guidelines issued by the Department of Defense (DoD) for its intelligence components.

7. ENVIRONMENT ASPECT AND IMPACT CONSIDERATIONS.

a. The development of this Manual and the general policies contained within it have been thoroughly reviewed by the originating office in conjunction with the Office of Environmental Management, Commandant (CG-47). This Manual is categorically excluded under current Department of Homeland Security (DHS) categorical exclusion (CATEX) A3 from further environmental analysis in accordance with "Implementation of the National Environmental Policy Act (NEPA)", DHS Instruction Manual 023-01-001-01 (series).

b. This Manual 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. All future specific actions resulting from the general policy in this Manual must be individually evaluated for compliance with the National Environmental Policy Act (NEPA), Department of Homeland Security (DHS) and Coast Guard NEPA policy, and compliance with all other applicable environmental mandates.

8. DISTRIBUTION. No paper distribution will be made of this Manual. An electronic version will be located on the following Commandant (CG-612) web sites.

Internet: http://www.dcms.uscg.mil/directives/ and

Coast Guard Portal: https://cg.portal.uscg.mil/library/directives/SitePages/Home.aspx

9. 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 does not produce any significant or substantial change to existing records management requirements.

10. APPLICABILITY. This Manual facilitates effective internal management of CGI NIE activities and does not create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies or entities, its officers, employees, or agents, or any other person. Within the Coast Guard only the NIE is authorized to conduct FI and CI activities pursuant to E.O. 12333. The Coast Guard NIE consists of only those intelligence elements and persons designated by the Assistant Commandant for Intelligence (CG-2) and which are subject to the National Security Act of 1947, E.O. 12333, and other authorities applicable to the Intelligence Community as defined in the National Security Act of 1947. This Manual only applies to CGI personnel when operating under NIE authorities. This Manual does not apply to CGI personnel when they are detailed or are assigned to Joint Duty Assignment (JDA)/TDY to other agencies; in those instances, CGI personnel are subject to the host agency's intelligence oversight rules and policies. Non-Coast Guard personnel detailed to CGI to execute national intelligence missions will comply with this Manual.

11. DOD APPLICABILITY. Coast Guard service members who are detailed to and assigned duties supervised by Department of Defense (DoD) intelligence components and who conduct DoD intelligence activity are subject to the issuance of Procedures Governing the Conduct of DoD Intelligence Activities, DoD Manual 5240.01 (series). When, pursuant to Presidential or Congressional action, the Coast Guard operates as a service in the Navy, the provisions of DoD Manual 5240.01 (series) will apply to all CGI NIE activity

12. MANUAL ORGANIZATION. This Commandant Instruction Manual (CIM) is organized into three parts. The first part establishes the purpose, aligns roles and responsibilities, and identifies authority for conducting FI and CI activities by the NIE. The second part – Appendix A – provides those Procedures (1-10), also known as Attorney General Guidelines, for the conduct of intelligence activities by the CGI NIE, and which are approved by the U. S. Attorney General. The third part – Appendix B – provides Coast Guard guidance for related activities and specific intelligence oversight aspects (Procedures 11-15), which do not require the Attorney General's approval. The Attorney General's approval of Procedures 1-10 is indicated by signature at the end of Appendix A (page A-59).

13. DEFINITIONS. See glossary section for each appendix for definition of words, statements, and acronyms.

14. FORMS/REPORTS. None.

15. REQUEST FOR CHANGES. Coast Guard NIE components must submit written requests for changes or amendments to this Manual through the chain of command to Commandant (CG- 25). Consideration for changes or amendments will be addressed in consultation with CG- LII.

16. EXCEPTIONS TO POLICY REQUESTS. Such requests must be made in writing via the chain of command to Commandant (CG-2) who must obtain the written concurrence of TJAG, through CG-LII and, if required, the Attorney General for any exceptions.

/ANDREW M. SUGIMOTO/
Rear Admiral, U.S. Coast Guard
Assistant Commandant for Intelligence

RECORD OF CHANGES			
CHANGE NUMBER	DATE OF CHANGE	DATE ENTERD	ENTERED BY

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A – ATTORNEY GENERAL GUIDANCE FOR COAST GUARD NATIONAL INTELLIGENCE ELEMENT (NIE) ACTIVITIES

A. Introduction.

This Appendix has been approved by the Attorney General, after consultation with the Director of National Intelligence (DNI), as required by Executive Order (E.O.) 12333.

B. Procedures.

These procedures are promulgated under E.O. 12333. The procedures set forth in this Appendix apply only to Coast Guard National Intelligence Element (NIE) personnel engaged in authorized intelligence activities or any other persons engaged in such activities on behalf of Coast Guard NIE. When, pursuant to Presidential or Congressional action, the Coast Guard operates as a service in the Navy, the Procedures Governing the Conduct of Department of Defense Intelligence Activities, DoD Manual (DoDM) 5240.01, rather than this Appendix, apply to all Coast Guard intelligence activities. DoDM 5240.01, rather than this Appendix, also applies to Coast Guard personnel (e.g., personnel in the Coast Guard Cryptologic Group) who are detailed to DoD and conducting DoD intelligence activities. Coast Guard personnel detailed to other Intelligence Community (IC) organizations must comply with the E.O. 12333 implementing procedures of that organization rather than this Appendix.

C. Interpretation.

The procedures in this Appendix will be interpreted in accordance with their stated purpose. All questions of interpretation will be referred to the Assistant Commandant for Intelligence (CG-2). Questions that cannot be resolved in this manner will be referred to the Coast Guard Judge Advocate General (TJAG), through the Chief, Information and Intelligence Law (CG-LII), who provides legal counsel to the Assistant Commandant for Intelligence (CG-2). As appropriate, Coast Guard privacy and civil liberties officials will be consulted. TJAG, after coordination with the Department of Homeland Security (DHS) Office of General Counsel (OGC), will consult with the Assistant Attorney General for National Security, as well as the Office of General Counsel of the Office of the Director of National Intelligence (ODNI), regarding any novel or significant interpretations of this Appendix and the potential applicability of IC Directive (ICD) 102.

D. Appendix Usage.

This Appendix is divided into different procedures related to the collection, use, retention, and oversight of foreign intelligence (FI) and counterintelligence (CI) within the Coast Guard NIE. Procedure 1 establishes the scope and administrative provisions for implementing this Appendix. Procedures 2 through 4 articulate the procedures through which Coast Guard NIE personnel are authorized to collect, retain, and disseminate U.S. person information (USPI). Procedures 5 through 10 govern the use of certain collection techniques to obtain information for FI and CI purposes. The Coast Guard NIE will employ the techniques governed by Procedures 5 through 10 only as necessary to perform authorized intelligence missions or functions assigned to the NIE.

E. References.

- Code of Federal Regulations, Title 39 (Postal Service)
- Executive Order 12333, "United States Intelligence Activities," as amended
- Executive Order 13462, "President's Intelligence Advisory Board and Intelligence Oversight Board," as amended
- Intelligence Community Directive 102, "Process for Developing Interpretive Principles and Proposing Amendments to Attorney General Guidelines Governing the Collection,

  Retention, and Dissemination of Information Regarding U.S. Persons," November 19, 2007, as amended
- Manual for Courts-Martial, United States (2019 Edition)
- Memorandum of Understanding Between the Department of Defense and Department of Justice, "Reporting of Information Concerning Federal Crimes," August 22, 1995
- Memorandum of Understanding Between the Federal Bureau of Investigation and the Department of Defense, "Governing Information Sharing, Operational Coordination and Investigative Responsibilities," August 2, 2011
- Public Law 113-293, "Intelligence Authorization Act for Fiscal Year 2015," December 19, 2014
- United States Code, Title 5, Section 552a, also known as "the Privacy Act of 1974"
- United States Code, Title 10 (Armed Forces)
- United States Code, Title 14 (Coast Guard)
- United States Code, Title 18 (Crimes and Criminal Procedure)
- United States Code, Title 50 (War and National Defense) (Chapter 36 is also known as "the Foreign Intelligence Surveillance Act (FISA)")
- United States Constitution, Amendments I, IV

PROCEDURE 1 – GENERAL PROVISIONS

A. Applicability and Scope.

1. The Coast Guard National Intelligence Element (hereinafter referred to as "the Coast Guard NIE" or "the NIE") provides necessary information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents. The procedures in this Appendix govern the conduct of the Coast Guard NIE, or anyone acting on behalf of the NIE or elements thereof, when conducting foreign intelligence (FI) or counterintelligence (CI) activities. Activities by the Coast Guard Law Enforcement Intelligence Element (LEIE) in support of law enforcement are not covered by the procedures in this Appendix.
2. This Appendix governs how the Coast Guard NIE will exercise its intelligence authorities and responsibilities, and does not confer any new authorities or responsibilities. Nothing in this Appendix shall be construed to authorize any activity in violation of the Constitution or statutes of the United States. The Coast Guard NIE may not investigate U.S. persons or collect or maintain information about them solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States. Coast Guard NIE personnel may neither undertake, nor solicit or request Coast Guard personnel who are not assigned to the Coast Guard NIE or third parties to undertake, any activity proscribed by applicable law, or contrary to E.O. 12333 or this Appendix.
3. Coast Guard NIE personnel must not conduct or provide support for covert actions, within the meaning of 50 U.S.C. § 3093, unless such actions have been directed by the President. Any Coast Guard participation in covert actions directed by the President must be consistent with E.O. 12333 and other applicable laws and directives.
4. National Intelligence Program funding must not be used for purposes other than those authorized by the National Security Act of 1947 or other statutes, E.O. 12333 or other Executive orders, Presidential directives, or IC policy.
5. All national intelligence activities must be conducted in accordance with applicable IC polices as promulgated by the DNI.
6. Coast Guard NIE personnel are not authorized to and will not engage in any intelligence activity, including dissemination to the White House, for the purpose of affecting the political process in the United States. Questions about whether a particular activity falls within this prohibition will be resolved in consultation with (i) the Command's legal officer, (ii) the Chief, Information and Intelligence Law (CG-LII), who is the legal counsel for the Assistant Commandant for Intelligence (CG-2), or (iii) TJAG.
7. Coast Guard NIE personnel will report a possible violation of federal criminal law by an employee or a possible violation of specified federal criminal laws by any other person, as required by Section 1.6(b) of E.O. 12333 and applicable policies. Reports must be made to the Coast Guard Investigative Service or TJAG.

8. When this Appendix requires a specific Coast Guard NIE official to approve an activity or take some other action, only that official (or person serving in that position in an acting capacity), or an official at a higher level in the chain of command, may take that action. When this Appendix permits an official to delegate authority for an action, the official may delegate the authority to one or more appropriate officials in accordance with NIE policy, unless specifically limited to a single delegee. All delegations must be in writing. Authority may not be redelegated unless expressly authorized in writing.

B. Shared Repositories.

1. *General*. The Coast Guard NIE may host or participate in a shared repository containing USPI only in accordance with this Appendix and applicable laws and policies. Each participant in a shared repository must comply with all laws, policies, and procedures applicable to the participant for the protection of USPI. Such participants may include Coast Guard elements that are not intelligence components, as well as entities outside Coast Guard when they participate in a shared repository hosted by the NIE.
2. *Coast Guard NIE Acting as Host.* The Coast Guard NIE acting as a host of a shared repository may perform systems support functions or data-related tasks (e.g., tagging, processing, or marking information) for itself or others. Access to USPI solely for these purposes does not constitute collection, retention, or dissemination pursuant to this Appendix. When the Coast Guard NIE acts as a host of a shared repository, it must enable auditing of access to USPI in the repository to the extent practicable.
3. *Coast Guard NIE Acting as a Participant.* The Coast Guard NIE acting as a participant in a shared repository must identify to the host any access and use limitations applicable to the USPI it provides. When the Coast Guard NIE provides USPI to a shared repository and allows access to or use of USPI by other participants, it has made a dissemination, which it may do only in accordance with Procedure 4 or other applicable Attorney General-approved guidelines. This does not include access to or use of USPI by a host or another element of the IC for systems support functions or data-related tasks.

C. Identification of National Intelligence Element Records for Oversight Purposes.

An NIE Record is any writing, paper, drawing, map, recording, photograph, tape, film, file, or other documentary material collected by the Coast Guard NIE in the course of intelligence activities governed by these procedures. The term includes any such documentary material stored by computer. The term does not include law enforcement intelligence or information related to administrative purposes.

All NIE Records must be identified and handled as such, as determined by the Assistant Commandant for Intelligence (CG-2), in a manner to distinguish them clearly from law enforcement intelligence (LEI) or non-intelligence information, in order to demonstrate the applicability of this Appendix to the records. Additionally, all NIE Records containing USPI must be clearly marked as determined by the Assistant Commandant for Intelligence (CG-2) in order to ensure compliance with this Appendix and applicable law, Executive orders, Presidential directives, and IC policies. Keeping or using unofficial files to avoid this requirement is prohibited.

D. Exceptions to Policy.

NIE personnel, through their chain of command, may submit written requests for exceptions to policy in this Appendix through the command's legal office to the Assistant Commandant for Intelligence (CG-2). In considering making requests for exceptions to policy, commanding officers should consult with their respective privacy and civil liberties officials.

1. Chief, Information and Intelligence Law (CG-LII) will present all requests for exceptions to policy to the Commandant Coast Guard (CCG), after consultation with TJAG and the DHS OGC. Exceptions to policy require the approval of the Assistant Attorney General for National Security after consultation with the DNI.
2. If time requirements constrain such review and approval, and an exception to these procedures is necessary due to the immediacy or gravity of a threat to the safety of persons, Coast Guard property, DHS property, other property over which the Coast Guard exercises regulatory authority, or the national security, the Assistant Commandant for Intelligence (CG-2) may approve an exception to these procedures. TJAG will be notified as soon thereafter as possible and TJAG will promptly deliver written notice of any such exceptions to the DHS OGC, the Assistant Attorney General for National Security, and the ODNI OGC. Activities in all circumstances must be carried out in accordance with the Constitution and laws of the United States.

E. Amendments.

NIE personnel, through their chain of command, may submit written requests for amendment to this Appendix through their servicing legal office to Chief, Information and Intelligence Law (CG-LII). In considering making requests for amendments, commanding officers should consult with their respective privacy and civil liberties officials. Chief, Information and Intelligence Law (CG-LII) will present all requests for amendments to the Assistant Commandant for Intelligence (CG-2) after consultation with TJAG and the DHS OGC. Substantive amendments, namely changes that are more than purely clerical corrections, require the approval of the Commandant Coast Guard (CCG) and the Attorney General, after consultation with the DNI. Non-substantive amendments such as correcting typographical errors or updating organizational titles and cross-references require the approval of the Assistant Commandant for Intelligence (CG-2) or designee, and notice to the National Security Division of the Department of Justice and ODNI OGC.

F. Internal Guidance.

This Appendix is published solely for internal Coast Guard guidance. It is not intended to, does not, and may not be relied on to create any rights, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person, nor does it place any limitation on otherwise lawful investigative and litigative prerogatives of the United States.

PROCEDURE 2 – COLLECTION OF U.S. PERSON INFORMATION (USPI)

A. Scope.

This procedure specifies the general criteria governing the collection of USPI. Only Paragraphs F. and G. apply to the acquisition of information in accordance with the Foreign Intelligence Surveillance Act (FISA), as amended, which is codified at Chapter 36 of Title 50, U.S.C.

B. Definition of Terms.

See the Glossary for the definitions of "administrative purposes," "agent of a foreign power," "communications security investigation", "counterintelligence (CI)," "collection," "consent," "cooperating sources," "dissemination," "domestic activities," "foreign connection," "foreign intelligence (FI)," "foreign power," "host of a shared repository," "imagery," "incidental collection of USPI," "Intelligence Community (IC) and elements thereof," "intentional collection of USPI," "international narcotics activities," "international terrorism or international terrorist activities," "National Intelligence Element (NIE)," "NIE personnel," "overhead reconnaissance," personnel security investigation," "publicly available information," "reasonable belief," "retention," "shared repository," "United States," "U.S. person," and "U.S. person information (USPI)."

C. Intentional Collection of USPI.

Intentional collection of USPI is authorized only if the information sought is reasonably believed to be necessary for the performance of an authorized intelligence mission or function assigned to the Coast Guard NIE, and if the USPI falls within one of the following categories:

1. *Publicly Available*. The information is publicly available.
2. *Consent*. The information concerns a U.S. person who has consented to such collection.
3. *Foreign Intelligence (FI)*. The information is reasonably believed to constitute FI and the U.S. person is:
    a. An individual reasonably believed to be an officer or employee of, or otherwise acting on behalf of, a foreign power;
    b. An organization or group reasonably believed to be directly or indirectly owned or controlled by, or acting on behalf of, a foreign power;
    c. An individual, organization, or group reasonably believed to be engaged in or preparing to engage in international terrorist or international narcotics activities;
    d. A corporation or other commercial organization reasonably believed to have some relationship with a foreign power, organization, or person;
    e. An individual reasonably believed to be a prisoner of war or missing in action; or
    f. An individual, organization, or group who is a target, hostage, or victim of an international terrorist or international narcotics organization.
4. *Counterintelligence (CI)*. The information is reasonably believed to constitute CI and the U.S. person is one of the following:

a. An individual, organization, or group reasonably believed to be engaged in or preparing to engage in espionage, other intelligence activities, sabotage, or assassination on behalf of a foreign power, organization, or person, or on behalf of an agent of a foreign power;

b. An individual, organization, or group reasonably believed to be engaged in or preparing to engage in international terrorist activities;

c. An individual, organization, or group reasonably believed to be acting for, or in furtherance of, the goals or objectives of an international terrorist or international terrorist organization, for purposes harmful to the national security of the United States; or

d. An individual, organization, or group in contact with a person described in Paragraphs C.4.a. through C.4.c. for the purpose of identifying such individual, organization, or group and assessing any relationship with the person described therein.

5. *Threats to Safety*. The information is needed to protect the safety of any person or organization, including those who are targets, victims, or hostages of international terrorist organizations. Coast Guard NIE personnel will only collect information that is needed to protect the safety of any person or organization if:

   a. The threat has a foreign connection;

   b. The Assistant Commandant for Intelligence (CG-2), or delegee, has determined that a person's life or physical safety is reasonably believed to be in imminent danger; or

   c. The information is needed to maintain maritime or aeronautical safety of navigation.

6. *Protection of Intelligence Sources, Methods, and Activities*. The information is about U.S. persons who have access to, had access to, will have access to, or are otherwise in possession of information that reveals FI or CI sources, methods, or activities, when collection is reasonably believed necessary to protect against the unauthorized disclosure of such information. Within the United States, Coast Guard NIE personnel will limit intentional collection of such information to persons who are:

   a. Current or former Coast Guard employees;

   b. Current or former employees of current or former Coast Guard contractors; or

   c. Applicants seeking employment with the Coast Guard or a Coast Guard contractor.

7. *Current, Former, or Potential Sources of Assistance to Intelligence Activities*. The information is about those who are or have been sources of information or assistance, or are reasonably believed to be potential sources of information or assistance, to intelligence activities for the purpose of assessing their suitability or credibility. This category does not include investigations undertaken for personnel security purposes.

8. *Persons in Contact With Sources or Potential Sources*. The information is about persons in contact with sources or potential sources, for the purpose of assessing the suitability or credibility of such sources or potential sources.

9. *Personnel Security*. The information is arising from a lawful personnel security investigation.

10. *Physical Security*. The information is arising from a lawful physical security investigation and is about U.S. persons reasonably believed to have a foreign connection and who pose a threat to the physical security of Coast Guard or DHS personnel, installations, operations, or visitors. Coast Guard NIE may also collect such information arising from and in the course of a lawful investigation resulting from a physical security inspection, vulnerability assessment, or reported security incident. In all cases, the Coast Guard NIE must have or be supporting an authorized physical security mission and must be able to articulate a reasonable belief in both the foreign connection of the U.S. persons who are collection targets and the physical security threat they pose.
11. *Communications Security Investigation*. The information is arising from a lawful communications security investigation.
12. *Overhead and Airborne Reconnaissance*. The information is obtained from overhead or airborne reconnaissance, including from unmanned aircraft systems and imagery from overhead or airborne collection platforms operated commercially or obtained from other sources.
    a. The Coast Guard NIE may intentionally collect imagery that contains USPI provided that the collection is not directed at a specific U.S. person or, if the collection is directed at a specific U.S. person, the collection falls in one of the other categories authorized by Paragraph C. of this procedure.
    b. Collection of any domestic imagery conducted by Coast Guard NIE must also comply with other applicable laws, policies, and procedures, including DoD or National Geospatial-Intelligence Agency (NGA) policies and procedures that govern such collection.
    c. All collection of imagery by the Coast Guard NIE must comply with constitutional and statutory requirements, Executive orders, Presidential directives, IC policies, and the other provisions of this Appendix.
13. *Administrative Purposes*. The information is required for administrative purposes.

D. Incidentally Collected USPI.

In the course of authorized collection activities, the Coast Guard NIE may incidentally collect USPI. This includes circumstances where the Coast Guard NIE has not deliberately sought the USPI, but entities or individuals on their own initiative voluntarily provide information to the Coast Guard NIE. All such information may be temporarily retained, evaluated for permanent retention, and disseminated only in accordance with Procedures 3 and 4. If an entity or individual is, on its own initiative, voluntarily providing on a recurring basis USPI that the Coast Guard NIE could not collect using other provisions of this procedure, the Coast Guard NIE will take appropriate steps to prevent such collection.

E. Special Circumstances Collection.

The Coast Guard NIE will consider whether collection opportunities raise special circumstances based on the volume, proportion, and sensitivity of the USPI likely to be acquired, and the intrusiveness of the methods used to collect the information. When special circumstances exist, the Assistant Commandant for Intelligence (CG-2) or delegee must consult with TJAG, appropriate officials

responsible for the protection of civil liberties and privacy, the Office of the Director of National Intelligence, and the National Security Division of the Department of Justice and determine whether to authorize the collection and, if so, whether enhanced safeguards are appropriate. If advance authorization is not possible, then as soon as possible after collection, the Assistant Commandant for Intelligence (CG-2) or delegee must determine whether to authorize the continued temporary retention of the information in accordance with Paragraphs E.1. and E.2., below, and Procedure 3. Any questions about whether special circumstances exist will be resolved in consultation with TJAG or the Chief, Information and Intelligence Law (CG-LII) and appropriate officials responsible for the protection of civil liberties and privacy, and in accordance with any subsequent guidance concerning implementation of this provision. An authorization of special circumstances collection will be based on both of the following:

1. The information will be or has been properly collected in accordance with Paragraph C. and the other provisions of this procedure; and
2. The collection activity is reasonable based on all the circumstances, including the value of the information; the collection methods used; the amount of USPI; the nature and sensitivity of the USPI; the civil liberties and privacy implications of the collection; the potential for substantial harm, embarrassment, inconvenience, or unfairness to U.S. persons if the USPI is improperly used or disclosed; and the safeguards that will be applied to the collected information in accordance with Procedure 3, Paragraph H.

F. General Criteria Governing the Means Used to Collect USPI.

1. *Means of Collection*. The Coast Guard NIE is authorized to collect USPI by any lawful means, provided that all such collection activities are carried out in accordance with E.O. 12333 and this Appendix.
2. *Restriction on Purpose*. The Coast Guard NIE may not collect USPI solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States.
3. *Least Intrusive Means*. The Coast Guard NIE will use the least intrusive collection techniques feasible within the United States or directed against U.S. persons abroad. In general, this means:
    a. To the extent feasible, such information will be collected from publicly available sources or with the consent of the person concerned.
    b. If collection from publicly available sources or obtaining consent from the person concerned is not feasible or sufficient, such information may be collected from cooperating sources.
    c. If collection from cooperating sources is not feasible or sufficient, such information may be collected using other lawful intelligence collection techniques that do not require a judicial warrant or the approval of the Attorney General.
    d. If collection in accordance with Paragraphs F.3.a. through F.3.c. is not feasible or sufficient, approval may be sought through TJAG, via Chief, Information and Intelligence Law (CG-LII), for the use of intelligence collection techniques that require a judicial

warrant or approval from the Attorney General.

4. *Amount of Information Collected*. In collecting USPI, the Coast Guard NIE will, to the extent practicable and after satisfying the criteria in Paragraph F.3., collect no more information than is reasonably necessary.

G. Limitations on the Collection of FI in the United States.

Collection of FI in the United States by the Coast Guard NIE is subject to the following limitations:

1. The Coast Guard NIE may collect FI concerning a U.S. person in the United States if:
   a. The information is publicly available; or
   b. The information is collected with the consent of the person concerned.
2. The Coast Guard NIE may collect FI concerning a U.S. person in the United States from a source who is advised, or is otherwise aware, that he or she is providing information to the U.S. Government if all of the following conditions are met:
   a. The FI cannot reasonably be obtained from publicly available information or with the consent of the person concerned;
   b. The FI sought is significant; and
   c. The collection is not undertaken for the purpose of acquiring information about any U.S. person's domestic activities.
3. The Coast Guard NIE may use sources or methods of collection in or directed at the United States, other than those authorized in Paragraphs G.1. and G.2., to collect FI, if all of the following conditions are met:
   a. The FI sought is significant;
   b. The collection is not undertaken for the purpose of acquiring information about any U.S. person's domestic activities;
   c. The FI cannot reasonably be obtained through the sources or methods authorized in Paragraphs G.1. and G.2.; and
   d. The Assistant Commandant for Intelligence (CG-2) or, when delegated, the Director, Coast Guard Counter Intelligence Service (CGCIS), has approved, as being consistent with this Appendix, the use of sources or methods other than those authorized in Paragraphs G.1. and G.2. The Assistant Commandant for Intelligence (CG-2) will immediately provide a copy of any such approval to TJAG.

PROCEDURE 3 – RETENTION OF U.S. PERSON INFORMATION (USPI)

A. Scope.

This procedure governs the retention of USPI collected by the Coast Guard NIE in accordance with Procedure 2. Information that does not fall within the definition of collection because it was disseminated by another element of the IC is subject to this procedure, except for Paragraphs C. and I. This procedure does not apply to the retention of information obtained under FISA, which has its own provisions.

B. Definition of Terms.

See the Glossary for the definitions of "administrative purposes," "collection," "consent," "counterintelligence (CI)," "dissemination," "foreign intelligence (FI)," "incidental collection of USPI," "Intelligence Community (IC) and elements thereof," "intentional collection of USPI," "National Intelligence Element (NIE)," "NIE personnel," "retention," "United States," "U.S. person," and "U.S. person information (USPI)."

C. Evaluation of Information.

The Coast Guard NIE will evaluate information that may contain USPI to determine whether it may be permanently retained under Paragraph E. as follows:

1. *Intentional Collection of USPI*. If the Coast Guard NIE intentionally collects USPI, it will evaluate the information promptly. If necessary, the Coast Guard NIE may retain the information for evaluation for up to 5 years. The Assistant Commandant for Intelligence (CG-2) or a single delegee may approve an extended period in accordance with Paragraph C.5.
2. *Incidental Collection of USPI*.
    a. **Collection about a person reasonably believed to be in the United States.** The Coast Guard NIE may intentionally collect information about a person or object that, at the time of collection, is in the United States or about a place in the United States. If, in the course of such collection, USPI may have been incidentally collected about a person other than the subject of the intentional collection, the incidentally collected information may be retained for evaluation for up to 5 years. The Assistant Commandant for Intelligence (CG-2) or a single delegee may approve an extended period in accordance with Paragraph C.5.
    b. **Collection about a person reasonably believed to be outside the United States.** The Coast Guard NIE may intentionally collect information about a person or object that, at the time of collection, is outside the United States or about a place outside the United States. If, in the course of such collection, USPI may have been incidentally collected about a person other than the subject of the intentional collection, the incidentally collected information may, subject to Paragraph F., be retained for evaluation for up to 25 years.
3. *Voluntarily Provided USPI*. If the Coast Guard NIE receives information that is voluntarily provided about a person reasonably believed to be a U.S. person, the information will be promptly evaluated. If necessary, the information may be retained for evaluation for up to 5 years. The Assistant Commandant for Intelligence (CG-2) or a single delegee may approve an

extended period in accordance with Paragraph C.5. If the Coast Guard NIE receives information that is voluntarily provided about a person reasonably believed to be a non-U.S. person, but the information may contain USPI, the information may, subject to Paragraph F., be retained for evaluation for up to 25 years.

4. *Special Circumstances*. If the Coast Guard NIE conducts a special circumstances collection in accordance with Procedure 2, Paragraph E., the information may be retained for evaluation for up to 5 years. If a special circumstances collection involves the intentional collection of USPI, that information will be promptly evaluated and, if necessary, may be retained for up to 5 years. The Assistant Commandant for Intelligence (CG-2) may approve an extended period in accordance with Paragraph C.5.

5. *Extended Retention*. The Assistant Commandant for Intelligence (CG-2) or a single delegee, as appropriate, may approve, either at the time of collection or thereafter, the further retention of specific information or categories of information subject to Paragraphs C.1., C.2.a., C.3., or C.4. for no more than 5 years beyond the time permitted in those paragraphs.

    a. The official must find that the retention is necessary to carry out an authorized mission of the Coast Guard NIE; find that the information will be retained and handled in a manner consistent with the protection of privacy and civil liberties; consider the need for enhanced protections, such as those described in Paragraph H.2., and consult with legal and privacy and civil liberties officials.

    b. In determining whether to approve an extended retention period, the official must also find that the information is likely to contain valuable information that the Coast Guard NIE is authorized to collect in accordance with Procedure 2.

    c. The official must document compliance with the requirements of this paragraph in writing. Any further extension of retention beyond the limits specified in Paragraph C. must be addressed as an exception to policy in accordance with Procedure 1, Paragraph D.

6. *Unintelligible Information*. For any information that is not in an intelligible form, the time periods identified in Paragraphs C.1 through C.4 begin when the information is processed into intelligible form. Unintelligible information includes information that Coast Guard NIE personnel cannot decrypt or understand in the original format. To the extent practicable, unintelligible information will be processed into an intelligible form.

7. *Deletion of Information*. Unless the Coast Guard NIE determines that USPI covered by Paragraph C. meets the standards for permanent retention during the specified time period, the Coast Guard NIE must delete all USPI (including any information that may contain USPI) from the Coast Guard NIE's automated systems of records.

D. Information Disseminated by Another IC Element.

If another element of the IC disseminates unevaluated information that may contain USPI to the Coast Guard NIE, the Coast Guard NIE may only retain the information and evaluate it for permanent retention pursuant to Paragraph E. for as long as the originating agency may retain it. If the disseminating IC element has already determined that the information meets the disseminating element's Attorney General approved standards for permanent retention, then the recipient must only verify that the information is reasonably believed to be necessary for the performance of the Coast

Guard NIE's authorized intelligence mission in order to permanently retain the information.

E. Permanent Retention.

1. *Retention Standard*. Subject to Paragraphs F., G., and H., the Coast Guard NIE may permanently retain USPI if it determines that retention is reasonably believed to be necessary for the performance of an authorized intelligence mission or function and the USPI falls into one or more of the following categories:
   a. The information was lawfully collected by the Coast Guard NIE or disseminated to the Coast Guard NIE by another element of the IC and meets a collection category in Procedure 2, Paragraph C.
   b. The information was lawfully collected by the Coast Guard NIE or disseminated to the Coast Guard NIE by another element of the IC, and is necessary to understand or assess FI or CI, such as information about a U.S. person that provides important background or context for FI or CI.
2. *Retention for Oversight*. The Coast Guard NIE may permanently retain USPI for the purposes of oversight, accountability, or redress when required to do so by law or court order or by direction from Chief, Information and Intelligence Law (CG-LII), TJAG, or the Attorney General.
3. *Retention of Specific USPI*. The Coast Guard NIE will determine whether information that contains USPI meets the standard for permanent retention at the most specific level of information that is appropriate and practicable.

F. Additional Requirements for "Covered Communications."

1. *Definitions*. For purposes of this paragraph and as defined in Section 309(a) of the Intelligence Authorization Act for Fiscal Year 2015 (codified at 50 USC § 1813), a "covered communication" is any nonpublic telephone or electronic communication acquired without the consent of a person who is a party to the communication, including communications in electronic storage, and "U.S. person" has the meaning given that term in 50 USC § 1801(i).
2. *Limitation on Extended Retention*. If the Coast Guard NIE acquires a covered communication as part of any intelligence collection activity not otherwise authorized by court order, subpoena, or similar legal process that is reasonably anticipated to result in the collection of such a communication to or from a U.S. person, the Coast Guard NIE may only retain the covered communication for more than five years if:
   a. The communication satisfies the requirements of one or more of the categories identified in Section 309(b)(3)(B) of the Intelligence Authorization Act for Fiscal Year 2015; and
   b. The Coast Guard NIE complies with any applicable approval and congressional reporting requirements.[1]

[1] It is also possible that another element of the IC may disseminate a covered communication to the Coast Guard NIE where the NIE has reason to believe either that the disseminating element has not made a determination that the information may be retained permanently in accordance with its Section 309 procedures or that the information is otherwise subject to reporting or other requirements imposed by the statute. The provisions of this paragraph also apply to

3. *Relationship to Other Provisions*. The requirements of this paragraph are in addition to the other requirements of this procedure. If this paragraph and the other requirements of this procedure have differing time periods for retaining information, then the shorter time period applies.

G. Protections for USPI.

1. *Responsibilities of the Coast Guard NIE*. The Coast Guard NIE will implement the following measures to protect USPI:
   a. Limit access to and use of such information to those employees who have appropriate security clearances, accesses, and a mission requirement.
   b. When retrieving information electronically:
      1) Only use queries or other techniques that are designed to retrieve information relevant to the intelligence mission or other authorized purposes.
      2) Tailor queries or other techniques to the greatest extent practicable to minimize the amount of USPI returned that is not pertinent to the intelligence mission and purpose for the query.
      3) Establish written procedures to document the basis for conducting a query of unevaluated information that is intended to reveal USPI.
   c. Take reasonable steps to audit access to information systems containing USPI and to periodically audit queries or other search terms to assess compliance with this Appendix.
   d. In developing and deploying information systems that are used for intelligence involving USPI, take reasonable steps to ensure effective auditing and reporting as required by this Appendix.
   e. Establish documented procedures for retaining data containing USPI, recording the reason for retaining the data, and identifying the authority approving the retention.
   f. In accordance with Coast Guard policy, annually train employees who access or use USPI on the civil liberties and privacy protections that apply to such information.
2. *Marking Electronic and Paper Files*. The Coast Guard NIE will use reasonable measures to identify and mark or tag files reasonably believed or known to contain USPI. Marking and tagging will occur regardless of the format or location of the information or the method of storing it. When appropriate and reasonably possible, NIE personnel will also mark files and documents containing USPI individually. In the case of certain electronic databases, if it is not reasonably possible to mark individual files containing USPI, the Coast Guard NIE may use a banner informing users before access that they may encounter USPI.
3. *Reviews*. Chief, Information and Intelligence Law (CG-LII) or other designated oversight personnel will periodically:

---

such a communication, with the five-year period beginning at the time when the other IC element first collected the communication.

a. Review Coast Guard NIE practices for protecting USPI in accordance with this procedure.

b. Evaluate the adequacy of temporary retention periods established in Paragraph C.

H. Enhanced Safeguards.

1. *Determining Need for Enhanced Safeguards*. Whenever there is a special circumstances collection in accordance with Procedure 2, Paragraph E., the Assistant Commandant for Intelligence (CG-2) or delegee will consider all of the following factors to assess whether there is a need for enhanced retention safeguards to protect USPI:

   a. The intrusiveness of the methods used by the Coast Guard or others to acquire the USPI.

   b. The volume, proportion, and sensitivity of the USPI being retained.

   c. The potential for substantial harm, embarrassment, inconvenience, or unfairness to U.S. persons if the USPI is improperly used or disclosed.

   d. The uses of the information being retained and the types of queries or searches expected to be conducted.

   e. The length of time the information may be retained.

   f. Practical and technical difficulties associated with implementing any enhanced safeguards.

   g. Any legal or policy restrictions that apply to the information, including Section 552a of Title 5, U.S.C., also known as "the Privacy Act of 1974."

   h. Other factors as directed by the Assistant Commandant for Intelligence (CG-2).

2. *Implementation of Enhanced Safeguards*. If the Assistant Commandant for Intelligence (CG-2) or delegee determines that there is a need for enhanced safeguards, he or she will consider and identify for implementation any of the following measures deemed appropriate:

   a. Procedures for review, approval, or auditing of any access or searches.

   b. Procedures to restrict access or dissemination, including limiting the number of personnel with access or authority to search; establishing a requirement for higher level approval or legal review before or after access or search; or requiring higher level approval or legal review before or after USPI is unmasked or disseminated.

   c. Use of privacy-enhancing techniques, such as information masking that indicates the existence of USPI without providing the content of the information, until the appropriate approvals are granted.

   d. Access controls, including data segregation, attribute-based access, or other physical or logical access controls.

   e. Additional training requirements.

   f. Additional protective retention measures, such as limiting the time for retention.

I. Maintenance and Disposition of Information.

The maintenance and disposition of USPI that is retained in Coast Guard NIE files will conform to this procedure and to the Coast Guard records management schedules approved by the Archivist of the United States for the files or records in which the information is retained.

J. Signals Intelligence (SIGINT).

Any retention of USPI obtained from SIGINT, including processing and querying of such USPI, is also subject to any annex to DoDM 5240.01 approved by the Attorney General (including any modification to the retention periods specified in DoDM 5240.01 made by the annex); policies and procedures promulgated in United States Signals Intelligence Directives (USSIDs) by the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS); and any applicable Presidential directives.

PROCEDURE 4 – DISSEMINATION OF U.S. PERSON INFORMATION (USPI)

A. Scope.

This procedure governs the dissemination of USPI collected or retained by the Coast Guard NIE. Information may be disseminated pursuant to this procedure only if it was properly collected or retained in accordance with Procedures 2 or 3. This procedure applies to USPI in any form, including physical and electronic files and information placed in databases, on websites, or in shared repositories accessible to other persons or organizations outside the Coast Guard NIE. This procedure does not apply to the dissemination of information collected solely for administrative purposes, or dissemination pursuant to other procedures approved by the Attorney General or a court order that otherwise imposes controls on such dissemination.

B. Definition of Terms.

See the Glossary for the definitions of "administrative purposes," "collection," "counterintelligence (CI)," "consent," "dissemination," "foreign intelligence (FI)," "Intelligence Community (IC) and elements thereof," "National Intelligence Element (NIE)," "NIE personnel," "publicly available information," "shared repository," "U.S. person," and "U.S. person information (USPI)."

C. Criteria for Dissemination.

USPI may be disseminated only by Coast Guard NIE personnel who have received training on this procedure and only if the information falls into one or more of the following categories and the dissemination complies with the other requirements in this procedure:

1. *Any Person or Entity*. The dissemination is to any person or entity and the information is publicly available or the information concerns a U.S. person who has consented to the dissemination.
2. *Other IC Elements*. The dissemination is to another appropriate element of the IC for the purpose of allowing the recipient to determine whether the information is relevant to its responsibilities and can be retained by it in accordance with its procedures approved by the Attorney General.
3. *Other Federal Government Entities*. The dissemination is to any other part of the federal government and the recipient is reasonably believed to have a need to receive such information for the performance of its lawful missions or functions.
4. *State, Local, Tribal, or Territorial (SLTT) Governments*. The dissemination is to a SLTT government and the recipient is reasonably believed to have a need to receive such information for the performance of its lawful missions or functions.
5. *Foreign Governments or International Organizations*. The dissemination meets all of the following requirements:
    a. The dissemination is to a foreign government or an international organization;
    b. The recipient is reasonably believed to have a need to receive such information for the performance of its lawful missions or functions; and

c. The Assistant Commandant for Intelligence (CG-2) or a delegee has determined that the disclosure is consistent with applicable international agreements or foreign partner sharing arrangements, and foreign disclosure policy and directives, including those policies and directives requiring protection against the misuse or unauthorized dissemination of information, and the analysis of potential harm to any identified individual.

6. *Assistance to the Coast Guard*. The dissemination is to a governmental entity, an international entity, or an individual or entity not part of a government and is necessary for the limited purpose of assisting the Coast Guard in carrying out an authorized mission or function. Any dissemination to a foreign government or international organization must also comply with Paragraph C.5. For a dissemination under this Paragraph C.6., the Assistant Commandant for Intelligence (CG-2), Director, CGCIS, Commanding Officer Intelligence Coordination Center (ICC), Commanding Officer Maritime Intelligence Fusion Centers (MIFCLANT and MIFCPAC), or their respective delegee, will inform the recipient that it should do all of the following, except in exceptional circumstances where providing such information is inconsistent with operational requirements as determined by the Assistant Commandant for Intelligence (CG-2) or a delegee:

   a. Only use the information for this limited purpose;

   b. Properly safeguard the information;

   c. Return or destroy the information when it has provided the requested assistance; and

   d. Not disseminate the information further without prior approval.

7. *Protective Purposes*. The dissemination is to a governmental entity, an international organization, or an individual or entity not part of a government, and is necessary to protect the safety or security of persons or property, or to protect against or prevent a crime or threat to national security. For any dissemination of USPI to individuals or entities not part of a government, the Assistant Commandant for Intelligence (CG-2), Deputy Assistant Commandant for Intelligence (CG-2d), Director, CGCIS, or a delegee identified by CG-2 will assess the risk associated with such dissemination, consider whether any further restrictions or handling caveats are needed to protect the information, and comply with any limitations required by foreign disclosure policy. Dissemination to a foreign government or international organization must also comply with Paragraph C.5.

8. *Required Disseminations*. The dissemination is required by statute; treaty; Executive order; Presidential directive; National Security Council guidance; policy, memorandum of understanding, or agreement approved by the Attorney General; or court order.

D. Disseminations of Large Amounts of Unevaluated USPI.

If the Coast Guard NIE wants to disseminate a large amount of USPI in accordance with Paragraphs C.3. through C.7. that has not been evaluated to determine whether it meets the standard for permanent retention, the Assistant Commandant for Intelligence (CG-2) or a single delegee must approve the dissemination after notifying TJAG.

1. The approving official must find that the dissemination complies with the other requirements of this procedure and that it is not reasonably possible to accomplish the intended objective by disseminating a lesser amount of USPI.
2. If the recipient is outside the federal government, the recipient must represent that it has appropriate protections in place, comparable to those required by Procedure 3, Paragraphs G. and H., to safeguard and monitor USPI and to comply with applicable laws; that it will use the information for lawful purposes; and that it will access and retain the information only for those purposes.

E. Minimization of Dissemination.

To the extent practicable, USPI should not be included in a dissemination (other than a dissemination pursuant to Paragraph C.1. or C.2.) if the pertinent information can be conveyed in an understandable way without including the USPI. If dissemination includes USPI, the disseminating entity will notify the recipient so the recipient can protect the USPI appropriately.

F. Disseminations Requiring Approval.

For any dissemination under Paragraphs C.3. through C.5. that is not for FI, CI, security, law enforcement, cybersecurity, humanitarian assistance, disaster relief, threats to safety, or protective purposes, the Assistant Commandant for Intelligence (CG-2) or delegee must approve the dissemination.

G. Dissemination of SIGINT.

The dissemination of information derived from SIGINT must also comply with the requirements of Procedure 5.

H. Improper Dissemination of USPI.

The Assistant Commandant for Intelligence (CG-2) will develop procedures to address instances of improper dissemination of USPI, including required reporting.

I. Dissemination Not Conforming to This Procedure.

Any proposed dissemination that does not conform to the requirements of this procedure must be approved by the Assistant Commandant for Intelligence (CG-2), after consultation with TJAG, the National Security Division of the Department of Justice, and relevant Coast Guard privacy and civil liberties officials. Such approval will be based on a determination that the proposed dissemination complies with applicable laws, Executive orders, Presidential directives, and IC policies.

PROCEDURE 5 – ELECTRONIC SURVEILLANCE

A. Scope.

The Coast Guard NIE may conduct electronic surveillance for an intelligence purpose or to support military operations. The legal framework for conducting electronic surveillance is dependent upon the Coast Guard's mission, the U.S. person status and location of the target, the methods used to conduct the electronic surveillance, and the type of communication sought. All electronic surveillance must comply with FISA or E.O. 12333, this procedure, and Procedures 1 through 4.

1. *Need for Guidance*. The authorities governing electronic surveillance are complex and subject to change. This procedure addresses the situations that most frequently arise and, even for those situations, only describes some of the legal requirements. Accordingly, Coast Guard NIE personnel should seek the guidance of legal counsel when planning and conducting electronic surveillance.
2. *Other Legal Authorities*. In addition to the legal authorities discussed below, other authorities are potentially applicable. For example, Sections 1841-1846 of Title 50, U.S.C., apply to the installation and use of pen register and trap and trace devices, which are devices used to obtain dialing, routing, addressing, or signaling information such as telephone numbers or e-mail addresses, and Title 18, U.S.C., contains a number of provisions that might apply depending on (among other things) the type and location of the surveillance or collection.
3. *Definition of Terms*. For the definitions of "agent of a foreign power," "collection," "counterintelligence (CI)," "consent," "dissemination," "electronic surveillance," "foreign intelligence (FI)," "foreign power," "incidental collection," "radio communications hearability survey," "reasonable expectation of privacy," "retention," "technical surveillance countermeasures (TSCM)," "transmission media vulnerability survey," "United States," "U.S. person," and "United States person information (USPI)," see the Glossary. In addition, for purposes of this procedure, the term "Attorney General" means the Attorney General, the Acting Attorney General, the Deputy Attorney General, and the Assistant Attorney General for National Security.

B. Compliance with the Fourth Amendment.

All electronic surveillance must comply with the Fourth Amendment to the Constitution. The Chief, Information and Intelligence Law (CG-LII), in consultation with TJAG, will assess the reasonableness of collection and restrictions on use, retention, and dissemination to ensure protection of Fourth Amendment rights and, when necessary, will consult with Coast Guard privacy and civil liberties officials and the National Security Division of the Department of Justice.

C. Electronic Surveillance Targeting a Person in the United States.

The Coast Guard NIE may conduct electronic surveillance targeting a person in the United States only for FI or CI purposes and in accordance with these procedures. FISA governs such activities, except in very limited circumstances.

1. *Legal References*. For FISA's applicability to electronic surveillance (as that term is defined in FISA) targeting a person in the United States, see Sections 101-112 of FISA (Sections 1801-1812 of Title 50, U.S.C.). Section 2.5 of E.O. 12333 may also apply to electronic surveillance targeting a person in the United States.
2. *Procedures*. Only the Attorney General or a judge of the Foreign Intelligence Surveillance Court (FISC) may authorize electronic surveillance, as that term is defined in FISA, targeting a person in the United States for intelligence purposes, except for certain emergency situations in accordance with Paragraph G. The Coast Guard NIE must comply with the requirements of FISA and, in most circumstances, may only conduct such surveillance if both:
    a. A significant purpose of the electronic surveillance is to obtain foreign intelligence information, as the terms "electronic surveillance" and "foreign intelligence information" are defined in FISA; and
    b. There is probable cause to believe that the target of the electronic surveillance is a foreign power or an agent of a foreign power, as the terms "electronic surveillance," "foreign power," and "agent of a foreign power" are defined in FISA.
3. *Authority to Request Electronic Surveillance Under This Paragraph*. Authority to approve the submission of applications or requests for electronic surveillance as that term is defined in FISA is limited to the Commandant Coast Guard (CCG), Vice Commandant Coast Guard (VCG), or the Assistant Commandant for Intelligence (CG-2). Applications to the FISC will be made through the Attorney General after being cleared by TJAG.

D. Electronic Surveillance Targeting a U.S. Person Outside the United States.

FISA and E.O. 12333 govern electronic surveillance conducted by the Coast Guard NIE targeting a U.S. person who is outside the United States.

1. *Legal References*. For electronic surveillance under FISA targeting a U.S. person outside the United States, see Sections 101-112, 703, 704, and 705 of FISA (Sections 1801-1812 and 1881b-d of Title 50, U.S.C.). Section 2.5 of E.O. 12333 also generally applies to electronic surveillance targeting a U.S. person outside the United States.
2. *Procedures*. When conducting electronic surveillance targeting a U.S. person outside the United States, the Coast Guard NIE must comply with both of the following, except to the extent specifically authorized under Paragraph H. of this procedure:
    a. The electronic surveillance must have been authorized under FISA or Section 2.5 of E.O. 12333, or both, as appropriate; and
    b. There must be probable cause to believe that the target of the electronic surveillance is a foreign power, an agent of a foreign power, or, in some circumstances, an officer or employee of a foreign power, as these terms are defined or otherwise set forth in FISA.
3. *Authority to Request Electronic Surveillance under This Paragraph*. Authority to approve the submission of applications or requests for electronic surveillance under FISA or Section 2.5 of E.O. 12333 is limited to the Commandant Coast Guard (CCG), Vice Commandant Coast Guard (VCG), or the Assistant Commandant for Intelligence (CG-2). Applications to the FISC

for orders are made through the Attorney General after being cleared by TJAG, via Chief, Information and Intelligence Law (CG-LII), except that applications for court orders pursuant to Sections 703, 704, or 705(a) of FISA (Sections 1881b, 1881c, and 1881d of Title 50, U.S.C.) may be submitted through the Attorney General after being cleared by the National Security Agency (NSA) OGC.

E. Electronic Surveillance under FISA Targeting a Non-U.S. Person Outside the United States.

1. *Procedures*. The Coast Guard NIE may request authorization for electronic surveillance targeting a non-U.S. person who is outside the United States under the following FISA authorities:

   a. **Section 702.** This Section of FISA may be used to obtain foreign intelligence information, as that term is defined in FISA, from or with the assistance of an electronic communication service provider, notwithstanding the requirements of Title I of FISA. The Coast Guard NIE may conduct electronic surveillance under Section 702 only in accordance with a joint certification from the Attorney General and the DNI, which certification is reviewed by the FISC. For information on electronic surveillance in accordance with Section 702, contact the NSA OGC or TJAG, through the Chief, Information and Intelligence Law (CG- LII). For additional information, see Section 702 of FISA (Section 1881a of Title 50, U.S.C).

   b. **Title I.** With the exception of electronic surveillance conducted under Section 702, title I of FISA applies if the Coast Guard NIE is seeking to conduct electronic surveillance as that term is defined in FISA. See Sections 101-112 of FISA (Sections 1801-1812 of Title 50, U.S.C.). The FISC or the Attorney General may approve an application or request for electronic surveillance of a foreign power or an agent of a foreign power, as those terms are defined in FISA, based on a finding that the application or request satisfies the requirements of FISA. See, e.g., Sections 102(a), 104(a), or 105 of FISA (Sections 1802(a), 1804(a), or 1805 of Title 50, U.S.C.).

2. *Authority to Request Title I Electronic Surveillance under This Paragraph*. Authority to approve the submission of applications or requests for electronic surveillance in accordance with Title I of FISA is limited to the Commandant Coast Guard (CCG), Vice Commandant Coast Guard (VCG), or the Assistant Commandant for Intelligence (CG-2). Applications to the FISC for court orders are made through the Attorney General after being cleared by TJAG.

F. Electronic Surveillance Under Executive Branch Authority.

The Coast Guard NIE may conduct electronic surveillance in accordance with this paragraph only for an authorized FI, CI, or support to military operations purpose. Such surveillance must be conducted in accordance with applicable law, E.O. 12333 and other Executive orders, Presidential directives, IC policies, and this Appendix. It may result in the incidental collection of USPI or the collection of communications to or from the United States. For collection under this paragraph, the Coast Guard will follow any annex to DoDM 5240.01 and applicable directives and instructions issued by DIRNSA/CHCSS governing the conduct of the U.S. SIGINT System.

G. Electronic Surveillance in Emergency Situations.

1. In accordance with FISA or Section 2.5 of E.O. 12333, the Coast Guard NIE may conduct electronic surveillance in emergency situations with the approval of the Attorney General. Authority to request emergency electronic surveillance is limited to the Commandant Coast Guard (CCG) or Vice Commandant (VCG). The Assistant Commandant for Intelligence (CG-2) or a delegee may request that TJAG seek authorization directly from the Attorney General if it is not feasible to submit such a request through one of these officials. Under this circumstance, the Assistant Commandant for Intelligence (CG-2) or a delegee will notify the appropriate official as soon as possible.
2. In addition, if the Coast Guard NIE is conducting electronic surveillance of a non-U.S. person outside the United States in accordance with Section 702 of FISA and that person enters the United States, under very limited circumstances the Commandant of the Coast Guard may authorize continued surveillance of that person for up to 72 hours in accordance with Section 105(f) of FISA (Section 1805(f) of Title 50, U.S.C.), with immediate notification to TJAG. Refer questions about this provision to the NSA OGC or TJAG.

H. Exigent Circumstances Involving a U.S. Person Outside the United States.

1. *Legal Standard*. The Coast Guard NIE may conduct electronic surveillance targeting a U.S. person outside the United States in exigent circumstances when securing the prior approval of the Attorney General is not practical and one or more of the following conditions exists:
   a. A person's life or physical safety is reasonably believed to be in imminent danger;
   b. The physical security of a defense installation or government property is reasonably believed to be in imminent danger; in this situation, the approving official must determine that there is probable cause to believe that the targeted U.S. person is a foreign power, an agent of a foreign power, or an officer or employee of a foreign power; or
   c. The time required would cause failure or delay in obtaining significant FI or CI, and such failure or delay would result in substantial harm to the national security. In this situation, the approving official must determine that there is probable cause to believe that the targeted U.S. person is a foreign power, an agent of a foreign power, or an officer or employee of a foreign power.
2. *Authority to Approve*. Authority to approve electronic surveillance involving exigent circumstances is limited to the Commandant Coast Guard (CCG), Vice Commandant Coast Guard (VCG), the Assistant Commandant for Intelligence (CG-2), or a single delegee designated by the Assistant Commandant for Intelligence (CG-2). Such official will promptly notify TJAG or the NSA OGC, as appropriate, of any such surveillance, the reason for authorizing the surveillance on an exigent basis, and the expected results. TJAG or the NSA OGC will notify the Attorney General as soon as possible of the surveillance, the circumstances surrounding its authorization, and the results thereof, and provide information as may be needed to authorize continuation of the surveillance.

3. *Time Limit*. Authorized electronic surveillance may continue for the amount of time required for a decision by the Attorney General, but may not continue for longer than 72 hours without the Attorney General's approval.

I. Electronic Surveillance Activities Subject to Special Provisions.

Coast Guard NIE personnel, if authorized, may in the normal course of their duties conduct electronic surveillance when:

1. *Testing the Capability of Electronic Equipment*.

   a. **Applicability.** Paragraph I.1. applies to testing the capability of electronic equipment that can intercept or process communications and non-communications signals. It implements the requirement for procedures under Section 105(g)(1) of FISA (Section 1805(g)(1) of Title 50, U.S.C.).

   b. **Signals That May Be Used Without Restriction.** The following signals may be used without restrictions, provided that their collection does not constitute electronic surveillance as that term is defined in FISA and is consistent with any other applicable federal surveillance statutes:

      1) Laboratory-generated signals, whether acquired inside or outside a laboratory.

      2) Communications signals acquired with the consent of one of the communicants.

      3) Communications in the commercial or public service broadcast bands.

      4) Communications transmitted between terminals located outside the United States not used by any known U.S. person.

      5) Non-communications signals.

   c. **Signals That May Be Used With Minimization Procedures**. Communications being collected in the course of lawful electronic surveillance in accordance with FISA or E.O. 12333 for FI or CI purposes may be used subject to the minimization procedures applicable to such surveillance.

   d. **Signals That May Only Be Used With the Restrictions Set Out in Paragraph I.1.e.:**

      1) Communications over official government communications circuits with consent from an appropriate official of the controlling agency, provided that their collection does not constitute electronic surveillance as that term is defined in FISA and is consistent with any other applicable federal surveillance statutes.

      2) Communications in the citizens and amateur-radio bands.

      3) Other signals may be used only when it is determined that it is not practical to use the signals described in Paragraphs I.1.d.1) and 2) and that it is not reasonable to obtain the consent of persons incidentally subjected to the surveillance. Use of such other signals to conduct electronic surveillance, as that term is defined in FISA, is authorized solely to test the capability of electronic equipment. The Attorney General must approve the use of signals pursuant to this paragraph when the period of use exceeds 90 days. When the Attorney General's approval is required, the Assistant Commandant for Intelligence

(CG-2) will submit a test proposal to the NSA OGC or TJAG. The test proposal will state the requirement for a test beyond 90 days, the nature of the activity, the organization that will conduct the activity, and the proposed disposition of any signals or communications acquired during the activity.

e. **Restrictions**.

1) **Scope.** The activities authorized in Paragraph I.1.d. will be limited in scope and duration to that necessary to determine the capability of electronic equipment.

2) **Targeting.** The activities will not target the communications of any particular person or persons.

3) **Retention, Use, and Dissemination.**

a. *Government Signals and Signals in the Citizens and Amateur-Radio Bands Collected under Paragraph I.1.d.1) and 2).* The technical parameters of a communication (e.g., frequency, modulation, bearing, signal strength, and time of activity) may be retained and used only for testing electronic equipment or for collection avoidance purposes. Technical parameters may be disseminated to other Coast Guard NIE components and to other entities authorized to conduct electronic surveillance or related testing of electronic equipment, provided that such dissemination and use are only for testing electronic equipment or for collection avoidance purposes. For purposes of this Paragraph I.1.e.3)a., the content of a communication is information about the substance, purport, or meaning of the communication. The content of a communication acquired in accordance with Paragraph I.1.d.1) or 2) may be retained or used only when needed for testing electronic equipment; may only be disclosed to persons conducting the activity; and must be destroyed before or immediately upon completion of the activity.

b. *Signals Collected under Paragraph I.1.d.3).* The technical parameters of a communication (e.g., frequency, modulation, bearing, signal strength, and time of activity), provided that they do not constitute content, may be retained and used only for testing electronic equipment or for collection avoidance purposes. Technical parameters not constituting content may be disseminated to other Coast Guard NIE components and to other entities authorized to conduct electronic surveillance or related testing of electronic equipment, provided that such dissemination and use are only for testing electronic equipment or for collection avoidance purposes. For purposes of this Paragraph I.1.e.3)b., the content of a communication is any information concerning the identity of the parties to the communication or the substance, purport, meaning, or existence of the communication, as the term “contents” is defined in Section 101(n) of FISA (Section 1801(n) of Title 50, U.S.C.). The content of a communication acquired pursuant to Paragraph I.1.d.3) may be retained or used only when needed to determine the capability of the electronic equipment; may be disclosed only to persons conducting the test; and must be destroyed before or immediately upon completion of the test.

4) **Compliance.** The activities authorized in Paragraph I.1.d. will be conducted in accordance with all legal requirements, including Sections 2510- 2523 of Title 18, U.S.C. (also known as the Wiretap Act), Sections 3121-3127 of Title 18, U.S.C. (also known as the Pen Register and Trap and Trace Devices Act), and FISA.

2. *Technical Surveillance Countermeasures (TSCM).*

a. **Applicability**. Paragraph I.2. applies to the use of electronic equipment and specialized techniques to determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance. It implements the requirement for procedures under Section 105(g)(2) of FISA (Section 1805(g)(2) of Title 50, U.S.C.).

b. **Procedures**. TSCM may only be conducted by the CGCIS. The use of TSCM equipment by CGCIS may involve the incidental acquisition of information, without consent, of those subjected to the surveillance, provided the use comports with all of the following conditions:

1) It is not reasonable to obtain the consent of persons incidentally subjected to the surveillance;

2) The TSCM is limited in extent and duration to that necessary to determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance;

3) The TSCM has been authorized or consented to by the official in charge of the facility, organization, or installation where the countermeasures are to be undertaken; and

4) If the TSCM constitutes electronic surveillance as that term is defined in FISA, such countermeasures are not targeted against the communications of any particular person or persons and the electronic surveillance is conducted solely to determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance.

c. **Retention, Use, and Dissemination of Information Acquired During TSCM Activities.**

1) In conducting TSCM, CGCIS may retain, use, or disseminate information that was acquired through electronic surveillance, as that term is defined in FISA, only in order to protect information from unauthorized surveillance or to enforce Chapter 119 of Title 18 or Section 605 of Title 47, U.S.C. Any information acquired must be destroyed when no longer required for these purposes or as soon as is practicable. CGCIS must also comply with Procedures 3 and 4.

2) The following types of information, if acquired in a manner that does not constitute electronic surveillance as that term is defined in FISA, may be retained and disseminated in accordance with Procedures 3 and 4 and Coast Guard Records Management Schedules:

a. The technical parameters of a communication (e.g., its frequency, modulation, bearing, signal strength, and time of activity);

b. A record of the types of communications and information subject to acquisition by unauthorized electronic surveillance that is detected by the TSCM; and

c. Any other information acquired in a manner that does not constitute electronic surveillance as that term is defined in FISA.

3. *Training of Coast Guard NIE Personnel in the Use of Electronic Surveillance Equipment*.

a. **Applicability.** This section applies to the training of Coast Guard NIE personnel in the use of electronic surveillance equipment. It implements the requirement for procedures under Section 105(g)(3) of FISA (Section 1805(g)(3) of Title 50, U.S.C.).

b. **Training Guidance.** The training of personnel in the use of electronic surveillance equipment will include guidance concerning the requirements and restrictions of FISA and E.O. 12333 with respect to the unauthorized acquisition and use of communications and information.

c. **Signals That May Be Used With Minimization Procedures**. Communications being collected in the course of lawful electronic surveillance in accordance with FISA or E.O. 12333 for FI or CI purposes may be used subject to the minimization procedures applicable to such surveillance.

d. **Preferred Signals for Training Purposes.** To the maximum extent practical, training in the use of electronic surveillance equipment will use and be directed against either (i) signals being collected in accordance with Paragraph I.3.c. or (ii) the following signals, provided that their collection does not constitute electronic surveillance as that term is defined in FISA and is consistent with any other applicable federal surveillance statutes:

1) Public broadcasts, distress signals, or official U.S. Government communications provided that, when government agency communications are monitored, the consent of an appropriate official is obtained.

2) Laboratory-generated signals, whether acquired inside or outside a laboratory.

3) Communications signals acquired with the consent of one of the communicants.

4) Communications transmitted between terminals located outside the United States not used by any known U.S. person.

5) Non-communications signals.

e. **Use of Other Signals for Training Purposes.** If it is not reasonable to train personnel in the use of electronic surveillance equipment using the signals described in Paragraphs I.3.c. or d as preferred signals for training purposes, the Coast Guard NIE may engage in electronic surveillance as that term is defined in FISA solely to train personnel in the use of electronic surveillance equipment if all of the following conditions are met:

1) The surveillance is not targeted against the communications of any particular person or persons;

2) It is not reasonable to obtain the consent of the persons incidentally subjected to the surveillance;

3) It is not reasonable to train personnel in the use of such equipment without engaging in electronic surveillance as that term is defined in FISA;

4) Such electronic surveillance is limited in extent and duration to that necessary to train the personnel in the use of the equipment; and

5) In training on the calibration of electronic surveillance equipment, as part of training on the use of that equipment, the acquisition of information is limited to that minimally necessary for calibration purposes.

f. **Retention, Use, and Dissemination**. Information collected during training that uses signals being collected in the course of lawful electronic surveillance for FI and CI purposes under Paragraph I.3.c. will be retained, used, and disseminated to the extent permitted by the applicable minimization procedures and will be maintained in accordance with Coast Guard Records Management Schedules. Information (including any information concerning the identity of the parties to a communication or the substance, purport, meaning, or existence of the communication) collected during training that uses signals collected under Paragraphs I.3.d. or e. (but excluding any signals collected pursuant to Paragraph I.3.c.) will be destroyed as soon as reasonably possible and may not be disseminated for any purpose. This limitation does not apply to distress signals.

J. Transmission Media Vulnerability and Radio Communications Hearability Surveys.

This paragraph applies to the conduct of transmission media vulnerability surveys and radio communications hearability surveys. If an activity falls within the definition of TSCM, it is governed by Paragraph I.2. and not this paragraph.

1. *Transmission Media Vulnerability Surveys*. With prior written authorization of the DIRNSA/CHCSS or a delegee, the Coast Guard NIE may conduct surveys of transmission facilities of communications common carriers, other private commercial entities, and U.S. Government entities to determine the potential vulnerability of the transmission media to interception by foreign intelligence services, subject to the following limitations:

   a. **Initiation of Collection.** When practicable, before a transmission media vulnerability survey begins, the Coast Guard NIE must obtain authorization or consent from the official in charge of the facility, organization, or installation where the survey is to be conducted.

   b. **Conduct of Surveys.** A transmission media vulnerability survey must be conducted as follows:

      1) Except as specified below, no content of any transmission may be collected by any means. For purposes of this Paragraph J.1., the content of a transmission is any information concerning the identity of the parties to the communication or the substance, purport, meaning, or existence of a communication.

         a. This limitation does not apply to the content of transmissions that are directed at or that may connect to a U.S. Government entity's facilities, when such transmissions are collected by that entity.

b. No transmission may be collected aurally, except for transmissions to or from U.S. Government entities acquired in accordance with other procedures approved by the Attorney General.

2) The survey must be conducted in accordance with all legal requirements, including Sections 2510-2523 of Title 18, U.S.C. (also known as the Wiretap Act), Sections 3121-3127 of Title 18, U.S.C. (also known as the Pen Register and Trap and Trace Devices Act), and FISA.

3) No transmissions may be recorded, except those authorized for collection in accordance with Paragraph J.1.b.1).

4) No report or log may include USPI, except for the purpose of identifying transmission facilities that are vulnerable to interception by foreign intelligence services. If the users of such facilities are not also the facilities' owners, the identities of the users may be obtained and may be included in a report or log. However, the identities of such users may not be obtained from the content of the transmissions, except for contents acquired in accordance with Paragraph J.1.b.1).

c. **Dissemination.** Reports may be disseminated in accordance with Procedure 4. Logs may be disseminated only if required to verify results contained in reports, and such dissemination must be in accordance with Procedure 4.

2. *Radio Communications Hearability Surveys*. With the prior written authorization of the DIRNSA/CHCSS or a delegee, the Coast Guard NIE may conduct radio communications hearability surveys of telecommunications that are transmitted in the United States, subject to the following limitations:

a. **Initiation of Collection.** When practicable, before a radio communications hearability survey begins, the personnel conducting the survey must obtain authorization or consent from the official in charge of the facility, organization, or installation where the survey is to be conducted.

b. **Conduct of Surveys**. A radio communications hearability survey must be conducted as follows:

1) The content of communications may not be recorded or included in any report or log. For purposes of this Paragraph J.2., the content of a communication is any information concerning the identity of the parties to the communication or the substance, purport, meaning, or existence of the communication.

2) The survey must be conducted in accordance with all legal requirements, including Sections 2510-2523 of Title 18, U.S.C. (also known as the Wiretap Act), Sections 3121-3127 of Title 18, U.S.C. (also known as the Pen Register and Trap and Trace Devices Act), and FISA.

3) No microwave transmission may be de-multiplexed or demodulated for any purpose.

4) No report or log may identify any person or entity, except for the purpose of identifying the transmission facility that can be intercepted from the intercept site. If the users of

such facilities are not also the facilities' owners, and the identities of the users are relevant to the purpose of the survey, the identities of the users may be obtained. However, neither the identities of the users or owners nor information about the existence of a specific communication may be obtained from the content of the transmissions themselves.

c. **Dissemination.** Reports may be disseminated in accordance with Procedure 4 and only within the U.S. government. Logs may be disseminated only if required to verify results contained in reports, and such dissemination must be in accordance with Procedure 4.

K. Military Tactical Exercise Communications.

These are U.S. and allied military exercise communications within the United States and abroad where collection, processing, retention, or dissemination of the communications is necessary either for the production of simulated FI or CI or to permit an analysis of communications security. The U.S. SIGINT System, including appropriate Coast Guard NIE components, may collect, process, retain, and disseminate military tactical exercise communications that contain USPI only in accordance with any annex to DoDM 5240.01.

1. *Collection*. Collection efforts will be conducted in the same manner as in the case of SIGINT for FI purposes and must be designed to avoid, to the extent feasible, the interception of communications not related to military exercises.
2. *Processing and Retention*.
   a. Military tactical exercise communications may be retained and processed without deletion of references to U.S. persons who are participants in, or are otherwise mentioned in, exercise-related communications.
   b. Inadvertently intercepted communications of U.S. persons or persons in the United States who are not participating in the exercise will be destroyed as soon as feasible in accordance with the Coast Guard's disposition schedule.
3. *Dissemination*. Dissemination of military tactical exercise communications and exercise reports or information files derived from such communications will be limited to those authorities and persons participating in, or conducting reviews and critiques of, such exercises.
4. *Consistency with Law.* These activities must be conducted in accordance with all legal requirements, including Sections 2510-2523 of Title 18, U.S.C. (also known as the Wiretap Act), Sections 3121-3127 of Title 18, U.S.C. (also known as the Pen Register and Trap and Trace Devices Act), and FISA.

PROCEDURE 6 – CONCEALED MONITORING

A. Scope.

1. This procedure governs concealed monitoring of any person inside the United States or any U.S. person outside the United States for an authorized FI or CI purpose by the CGCIS.
2. Only CGCIS is authorized to conduct concealed monitoring for the Coast Guard.
3. This procedure does not apply to concealed monitoring conducted as part of testing or training exercises when the subjects are participants who have consented to the concealed monitoring as part of an approved testing or training plan. CGCIS may, however, collect, retain, and disseminate USPI in the course of such concealed monitoring only if otherwise authorized by this Appendix.
4. This procedure does not apply if the monitoring device is used in circumstances in which a person being monitored has a reasonable expectation of privacy. The installation or use of any monitoring device in the United States in circumstances in which a person has a reasonable expectation of privacy, as determined by TJAG or the Chief, Information and Intelligence Law (CG-LII), and a warrant would be required for law enforcement purposes is electronic surveillance (as that term is defined in FISA) and is, as a result, subject to Procedure 5. The use of a monitoring device in such circumstances against a U.S. person outside the United States is also subject to Procedure 5.

B. Definition of Terms.

See the Glossary for the definitions of "counterintelligence (CI)," "Coast Guard facilities," "concealed monitoring," "collection," "consent," "dissemination," "electronic surveillance," "foreign intelligence (FI)," "reasonable expectation of privacy," "retention," "United States," "U.S. person," and "U.S. person information (USPI)."

C. Procedures.

CGCIS may conduct concealed monitoring only as follows:

1. *In the United States*. CGCIS may conduct concealed monitoring on a Coast Guard facility. CGCIS may conduct concealed monitoring outside Coast Guard facilities after coordination with the Federal Bureau of Investigation (FBI) and in accordance with any applicable agreements with the Department of Justice or the FBI. Monitoring is in the United States if the monitoring device or a subject of the monitoring is located in the United States.
2. *Outside the United States*. CGCIS may conduct concealed monitoring on a Coast Guard facility. Monitoring outside Coast Guard facilities must be coordinated with the Central Intelligence Agency (CIA), and appropriate host country officials in accordance with any applicable Status of Forces Agreement (SOFA) or other international agreement.
3. *Approval for Concealed Monitoring That Occurs in the United States or That Is Directed Against a U.S. Person Outside the United States*. Concealed monitoring in the United States or directed against a U.S. person outside the United States must be approved by the Assistant Commandant for Intelligence (CG-2) or a delegee, after consultation with

TJAG. TJAG or the Chief, Information and Intelligence Law (CG-LII) will determine whether a person has a reasonable expectation of privacy. For monitoring that occurs outside the United States, the Assistant Commandant for Intelligence (CG-2) must also consider the laws and policies of the host government and any applicable SOFA or international agreement. Approval of the concealed monitoring will be based on a determination that all of the following criteria have been met:

a. There is no reasonable expectation of privacy;

b. Such monitoring is necessary to conduct an assigned FI or CI function;

c. A trespass will not be necessary to effect the monitoring; and

d. The monitoring is not subject to Procedure 5.

PROCEDURE 7 – PHYSICAL SEARCHES

A. Scope.

This procedure applies to physical searches for FI or CI purposes of any person or property in the United States and of U.S. persons or their property outside the United States. Only CGCIS is authorized to conduct physical searches for the Coast Guard NIE under this Procedure. (Note that consensual searches of a person or property are governed by Procedure 2 and not this Procedure.)

B. Definition of Terms.

See the Glossary for the definitions of "counterintelligence (CI)," "consent," "domestic activities," "foreign intelligence (FI)," "National Intelligence Element (NIE)," "physical search," "United States," and "U.S. person."

C. Physical Searches Directed Against Active-Duty Military Personnel or Their Property.

1. *Limitations*. Only CGCIS is authorized to conduct physical searches directed against active-duty military personnel or their property for FI or CI purposes. The Attorney General or the FISC must approve such searches conducted inside or outside the United States in accordance with, as applicable, Sections 301-309, 703, 704, or 705 of FISA (Sections 1821-1829, 1881b, 1881c, or 1881d of Title 50, U.S.C.) or Section 2.5 of E.O. 12333.
2. *Authority to Request Searches*. Only the Commandant Coast Guard (CCG), Vice Commandant Coast Guard (VCG), or Assistant Commandant for Intelligence (CG-2) may seek approval for physical searches described in Paragraph C.1. Applications for court orders will be made through the Attorney General after being cleared by TJAG.
3. *Emergencies*. The Deputy Assistant Commandant for Intelligence (CG-2d) or Director, CGCIS may request that TJAG seek authorization directly from the Attorney General in an emergency if it is not feasible to submit such a request through an official designated in Paragraph C.2., provided that the appropriate official is notified as soon as possible thereafter.

D. Physical Searches Directed Against Other Persons or Property in the United States.

1. *Limitations*. Except for searches directed against active-duty military personnel or their property authorized in accordance with Paragraph C., CGCIS may not conduct a physical search of any person or property in the United States for an FI or CI purpose. This includes both U.S. and non-U.S. persons. These searches will be conducted by the FBI. The CGCIS Director may request the FBI to conduct such a search, and request that CGCIS agents be present during the search, if both of the following conditions are met:
   a. The search is for an authorized FI or CI purpose and, if directed at a U.S. person for an FI purpose, the FI sought is significant and the search is not being undertaken to obtain information about the domestic activities of any U.S. person; and
   b. The search meets the definition of a physical search in FISA, and satisfies the requirements of FISA for such searches.

2. *Authority to Request Searches*. Requests made by the Director, CGCIS to conduct a physical search under Paragraph D.1. must be approved by the Assistant Commandant for Intelligence (CG-2). Applications for court orders will be made through the Attorney General after being cleared by TJAG.

3. *Emergencies*. Upon the approval of the Deputy Assistant Commandant for Intelligence (CG-2d), and with the concurrence of TJAG or a single delegee, the Director, CGCIS may request the FBI to conduct a physical search in accordance with Paragraph D.1. in an emergency if it is not feasible to submit such a request through an official designated in Paragraph D.2., provided that the appropriate official is notified as soon as possible thereafter. The FBI must obtain the authorization of the Attorney General in accordance with FISA.

E. Physical Searches Directed Against Other U.S. Persons or Their Property Outside the United States.

1. *Requirements*. CGCIS, with the approval of the Assistant Commandant for Intelligence (CG-2) and the concurrence of TJAG, may conduct a physical search directed against a U.S. person outside the United States who is not an active-duty service member, or of property located outside the United States of any U.S. person who is not an active-duty service member, if all of the following conditions are met:

   a. The search is for an authorized FI or CI purpose;

   b. The search is appropriately coordinated with the CIA; and

   c. The FISC or the Attorney General has authorized the search in accordance with, as applicable, Sections 703, 704, or 705 of FISA (Sections 1881b, 1881c, or 1881d of Title 50, U.S.C.) or Section 2.5 of E.O. 12333.

2. *Authority to Request Searches*. Only the Commandant Coast Guard (CCG), Vice Commandant Coast Guard (VCG), or Assistant Commandant for Intelligence (CG-2) may seek approval for physical searches in accordance with Paragraph E.1. Applications for court orders will be made through the Attorney General after being cleared by TJAG.

3. *Emergencies*. Upon the approval of the Deputy Assistant Commandant for Intelligence (CG-2d), with the concurrence of TJAG or a single delegee, CGCIS may conduct a physical search in accordance with Paragraph E.1. in an emergency with the authorization of the Attorney General. The Deputy Assistant Commandant for Intelligence (CG-2d) or the Director, CGCIS may request that TJAG seek authorization directly from the Attorney General, if it is not feasible to submit such a request through an official designated in Paragraph E.2., provided that the appropriate official is notified as soon as possible thereafter.

PROCEDURE 8 – SEARCHES OF MAIL AND THE USE OF MAIL COVERS

A. Scope.

This procedure governs the physical searches of mail, including the opening or other examination of the content of mail, in the United States and abroad, by the Coast Guard NIE or anyone acting on its behalf. This procedure also applies to the use of mail covers. Only CGCIS is authorized to conduct searches of mail and use mail covers, and these activities must be for authorized FI or CI purposes. This procedure does not apply to items transported by a commercial carrier (e.g., Federal Express or the United Parcel Service). Such items are subject to the provisions of Procedure 7. (Note that consensual searches of a person or property are governed by Procedure 2 and not this Procedure or Procedure 7.)

B. Definition of Terms.

See the Glossary for the definitions of "counterintelligence (CI)," "foreign intelligence (FI)," "mail in USPS channels," "mail cover," "National Intelligence Element (NIE)," "physical search," "United States," and "U.S. person."

C. Physical Searches of Mail.

1. *Mail in the United States – Active-Duty Military Personnel*. CGCIS may conduct a physical search of the mail of active-duty military personnel for FI or CI purposes when such mail is in the United States. CGCIS may request assistance from the United States Postal Service (USPS) to conduct the search. All such searches must comply with the following requirements:

   a. **Limitations**. The Attorney General or the FISC must approve such searches conducted inside the United States in accordance with Sections 301 to 309 of FISA (Sections 1821-1829 of Title 50, U.S.C.).

   b. **Authority to Request Searches**. Only the Commandant Coast Guard (CCG), Vice Commandant Coast Guard (VCG), or the Assistant Commandant for Intelligence (CG-2) may seek approval for searches described in Paragraph C.1. Applications for court orders will be made through the Attorney General after being cleared by the Assistant Commandant for Intelligence (CG-2), with the concurrence of TJAG.

   c. **Emergencies**. The Deputy Assistant Commandant for Intelligence (CG-2d) or Director, CGCIS may request that TJAG seek authorization directly from the Attorney General in an emergency if it is not feasible to submit such a request through an official designated in Paragraph C.1.b., provided that the appropriate official is notified as soon as possible thereafter.

2. *Mail in the United States -- Other Persons in the United States.*

   a. **Limitations.** Except for searches directed against active-duty military personnel authorized in accordance with Paragraph C.1., the Coast Guard NIE, including CGCIS, may not conduct physical searches of mail in the United States for FI or CI purposes. This includes mail of both U.S. and non-U.S. persons. These searches will be conducted by the FBI. The Director, CGCIS may request the FBI to conduct such a search, and request that CGCIS

agents be present during the search, if both of the following conditions are met:

1) The search is for an authorized FI or CI purpose and, if directed at a U.S. person for an FI purpose, the FI sought is significant and the search is not being undertaken to obtain information about the domestic activities of any U.S. person.

2) The search meets the definition of a physical search in FISA, and satisfies the requirements of FISA for such searches.

b. **Authority to Request Searches.** Requests made by the Director, CGCIS to conduct a mail search under Paragraph C.2.a. must be approved by the Assistant Commandant for Intelligence (CG-2). Applications for court orders will be made through the Attorney General, after being cleared by TJAG.

c. **Emergencies**. Upon the approval of the Deputy Assistant Commandant for Intelligence (CG-2d), and with the concurrence of TJAG or a single delegee, the Director, CGIS may request the FBI to conduct a mail search in accordance with Paragraph C.2.a. in an emergency if it is not feasible to submit such a request through an official designated in Paragraph C.2.b., provided that the appropriate official is notified as soon as possible thereafter. The FBI must obtain the authorization of the Attorney General in accordance with FISA.

3. *Mail outside the United States – Active-Duty Military Personnel*. CGCIS may conduct a physical search of the mail of active-duty personnel who are outside the United States for CI purposes when such mail is also outside the United States, provided that the search complies with the following:

a. **Limitations.** The Attorney General or the FISC must approve such searches conducted outside the United States in accordance with Sections 704 or 705 of FISA (Sections 1881c or 1881d of Title 50, U.S.C.).

b. **Authority to Request Searches under FISA.** The Director, CGCIS may seek approval for physical searches described in Paragraph C.3. Applications for court orders will be made through the Attorney General after being cleared by the Assistant Commandant for Intelligence (CG-2) or a delegee, with the concurrence of TJAG.

c. **Emergency Searches under FISA.** The Assistant Commandant for Intelligence (CG-2), or a delegee, on behalf of the Director, CGCIS, may request that TJAG seek authorization directly from the Attorney General in an emergency, if it is not feasible to submit such a request through an official designated in Paragraph C.3.b., provided that the appropriate official is notified as soon as possible thereafter.

4. *Mail outside the United States – Other Persons*. After appropriate coordination with the CIA and host nation authorities, CGCIS may conduct a physical search (or request the USPS to conduct a physical search) of mail outside the United States of other U.S. persons or non- U.S. Persons (wherever located), provided that CGCIS complies with any applicable host nation law, SOFA, or other international agreement and that any physical search of the mail of such a U.S. person is approved as follows:

a. **Requirements.** CGCIS, with the approval of the Assistant Commandant for Intelligence

(CG-2) or a delegee, may conduct a physical search of the mail of a U.S. person outside the United States if both of the following conditions are met:

i. The search is for an authorized FI or CI purpose; and

ii. The FISC or the Attorney General has authorized the search in accordance with, as appropriate, Sections 704 or 705 of FISA (Sections 1881c or 1881d of Title 50, U.S.C.) or Section 2.5 of E.O. 12333.

b. **Authority to Request Searches.** The Director, CGCIS may seek approval for mail searches described in Paragraph C.4.a. Applications for court orders will be made through the Attorney General after being cleared by the Assistant Commandant for Intelligence (CG-2), with the concurrence of TJAG.

c. **Emergencies**. Upon the approval of the Assistant Commandant for Intelligence (CG-2), the Director, CGCIS may conduct a mail search described in Paragraph C.4.a. in an emergency with the authorization of the Attorney General. The CGCIS Director may request such authorization directly from the Attorney General, if it is not feasible to submit such a request through an official designated in Paragraph C.4.b., provided that TJAG and the appropriate official are notified as soon as possible thereafter.

5. *Compliance with U.S. Postal Service Regulations*. In addition to complying with the other requirements of Paragraph C., all physical searches of mail in USPS channels must comply with applicable postal regulations. This applies to mail both in and outside the United States.

D. Mail Covers.

1. CGCIS may for FI or CI purposes, upon the approval of the Assistant Commandant for Intelligence (CG-2), with the concurrence of TJAG, request the USPS to use a mail cover for mail in USPS channels in accordance with Section 233.3(e)(2) of Title 39, Code of Federal Regulations.

2. For mail that is in foreign postal channels, CGCIS may for FI or CI purposes, upon the approval of the Assistant Commandant for Intelligence (CG-2), with the concurrence of TJAG, request a mail cover for mail that is to or from a U.S. person consistent with appropriate law and procedure of the foreign government and the provisions of any applicable SOFA or international agreement.

PROCEDURE 9 – PHYSICAL SURVEILLANCE

A. Scope.

1. This procedure governs physical surveillance of any person inside the United States or any U.S. person outside the United States by the Coast Guard NIE or anyone acting on its behalf. Only CGCIS is authorized to conduct physical surveillance of U.S. persons to collect FI or CI. If CGCIS or anyone acting on its behalf is conducting physical surveillance, this procedure applies to any devices such person is operating to observe the subject of the surveillance, and not the provisions of Procedure 6.
2. This procedure does not apply to physical surveillance conducted as part of testing or training exercises when the subjects are participants in an exercise who have consented to the surveillance as part of an approved testing or training plan.
3. It also does not apply to surveillance detection or counter surveillance activities in which CGCIS personnel must detect and elude foreign physical surveillance. CGCIS may, however, collect, retain, and disseminate USPI in the course of such surveillance detection or counter surveillance activities only if otherwise authorized by this Appendix.

B. Definitions of Terms.

See the Glossary for the definitions of "counterintelligence (CI)," "collection," "consent," "cooperating sources," "detail," "dissemination," "foreign intelligence (FI)," "National Intelligence Element (NIE)," "physical surveillance," "retention," "United States," "U.S. person," and "United States person information (USPI)."

C. Procedures.

1. *Physical Surveillance in the United States*.
   a. **U.S. Persons in the United States.** With Assistant Commandant for Intelligence (CG-2) approval and TJAG concurrence, CGCIS may conduct physical surveillance for an authorized FI or CI purpose of any U.S. person in the United States who is (i) a present or former military or civilian employee of the Coast Guard NIE; (ii) a present or former contractor of the Coast Guard NIE or a present or former employee of such a contractor; (iii) an applicant for any such employment or contracting; (iv) a military service member employed by a non-intelligence element of the military; or (v) an individual who is a present or former cooperating source who is or was acting for the Coast Guard NIE and who has consented to the physical surveillance.
   b. **Non-U.S. Person in the United States.** CGCIS, with concurrence of CGCIS legal counsel, may conduct physical surveillance of a non-U.S. person in the United States for an authorized FI or CI purpose.
   c. **Coordination with Law Enforcement Agencies.** CGCIS must coordinate any physical surveillance in the United States with the FBI and, if appropriate, with other law enforcement agencies, unless the surveillance is of an active-duty military person while on a military installation. CGCIS personnel may only participate in physical surveillance in

the United States of U.S. persons other than those in the categories identified in Paragraph C.1.a when detailed to the FBI, including during joint investigative or operational activity.

d. **Participation with the FBI.** In addition to physical surveillance conducted in accordance with Paragraphs C.1.a. and C.1.b., the Assistant Commandant for Intelligence (CG-2), or a delegee, may approve CGCIS participation in an authorized FBI FI or CI physical surveillance operation in the United States when Coast Guard or DHS equities are involved. The FBI must request and authorize such participation in writing.

2. *Physical Surveillance Outside the United States*.

a. **Criteria.** Only CGCIS may conduct physical surveillance of any U.S. person who is outside the United States and may do so only for an authorized FI or CI purpose.

b. **Limitation on Foreign Intelligence Collection.** Physical surveillance of a U.S. person outside of the United States to collect FI may only be authorized to obtain significant information that cannot reasonably be acquired by other means.

c. **Required Coordination and Approval Authority.** Upon approval of the Assistant Commandant for Intelligence (CG-2) or a delegee, and with the concurrence of TJAG, the Director, CGCIS may approve physical surveillance outside of the United States of any U.S. person for an authorized FI or CI purpose. Physical surveillance outside of the United States, with the exception of physical surveillance on a military installation, must be coordinated with the CIA. The approving official must consider the laws and policies of the host government and any applicable SOFA or international agreement.

PROCEDURE 10 – UNDISCLOSED PARTICIPATION (UDP) IN ORGANIZATIONS

A. Scope.

This procedure governs the undisclosed participation by Coast Guard NIE personnel and anyone, including sources, acting on behalf of the Coast Guard NIE in any organization in the United States or any organization outside the United States that constitutes a U.S. person.

B. Definition of Terms.

See the Glossary for the definitions of "NIE personnel," "counterintelligence (CI)," "collection," "domestic activities," "foreign intelligence (FI)," "foreign power," "intelligence activities," "organization," "organization in the United States," "organization outside the United States that constitutes a U.S. person," "participation in an organization," "publicly available information," "undisclosed participation (UDP)," "United States," "U.S. person," and "U.S. person information (USPI)."

C. Exclusions.

This procedure does not apply to:

1. *Personal Participation*. Activities conducted within an organization solely for personal purposes (i.e., activities undertaken upon the initiative and at the expense of a person solely for personal benefit).
2. *Voluntarily Provided Information*. Activities conducted within an organization by any person who is already a member of the organization, or who joins on his or her own behalf, and later volunteers information to the Coast Guard NIE not in response to a request or tasking by the Coast Guard NIE or another element of the IC.
3. *Publicly Available Information on the Internet*. Collection of publicly available information on the internet in a way that does not require a person to provide identifying information (such as an email address) as a condition of access and does not involve communication with a human being.
4. *Classes*. Attendance by Coast Guard NIE personnel or anyone acting on behalf of the Coast Guard NIE at commercial classes or training on non-intelligence skills, when under no direction or tasking to collect intelligence, and the attendee's true name and Coast Guard NIE affiliation is used.
5. *Professional Skills*. Participation in educational or professional organizations to enhance professional skills, knowledge, or capabilities of employees, when under no direction or tasking to collect intelligence, and the employee's true name and Coast Guard NIE affiliation is used.

D. General Requirement.

Anyone acting on behalf of the Coast Guard NIE may join, become a member of, or otherwise participate in an organization in the United States, or in any organization outside the United States that constitutes a U.S. person, if his or her intelligence affiliation is disclosed to an appropriate official of

the organization in accordance with Paragraph G. Without such disclosure, the other provisions of this procedure must be applied to authorize UDP.

E. Limitations on UDP.

1. *Lawful Purpose*. All UDP must be essential to achieving a lawful FI or CI purpose, as determined by the Assistant Commandant for Intelligence (CG-2) or delegee, within the assigned mission of Coast Guard NIE.
2. *Domestic Activities*. UDP may not be authorized for the purpose of collecting information on the domestic activities of U.S. persons.
3. *Coordination.* All UDP must be coordinated with the FBI, CIA, or any other appropriate agency in accordance with E.O. 12333 and applicable policy and agreements.
4. *UDP for FI Purposes in the United States*. UDP may not be authorized in the United States to collect FI from or about a U.S. person, or to collect information necessary to assess a U.S. person as a potential source of assistance to FI activities. This limitation does not preclude the collection of information about such persons, when volunteered by sources participating in an organization to which such persons belong, if otherwise permitted by Procedure 2.
5. *Duration of UDP*. Authorization to conduct UDP that requires specific approval under this procedure will be limited to the duration of the intelligence activity it is supporting or 12 months, whichever is shorter. If specific approval is required by this procedure, an appropriate official must review and re-approve participation for more than 12 months on an annual basis in accordance with this procedure.
6. *Participation for the Purpose of Influencing the Activities of an Organization or Its Members*.
    a. UDP is not authorized for the purpose of influencing the activities of an organization within the United States, or any organization outside the United States that constitutes a U.S. person, or the members of such organizations, unless either:
        1) Such participation is undertaken on behalf of the FBI in the course of a lawful investigation, or
        2) The organization concerned is composed primarily of individuals who are non-U.S. persons and the organization is reasonably believed to be acting on behalf of a foreign power.
    b. The Coast Guard NIE, if it desires to have a person acting on its behalf engage in UDP for such purposes, will forward its request to the Assistant Commandant for Intelligence (CG-2) and TJAG, via the chain of command, for approval, setting forth the relevant facts justifying such participation and explaining the nature of its contemplated activity.
    c. In the case of an organization outside the United States that constitutes a U.S. person, the prohibition on influencing the activities of an organization's members does not apply to non-U.S. persons who are members located outside the United States, provided that the approving authority has considered the possible impact on domestic activities.

F. Required Approvals.

Subject to the limitations of Paragraph E., UDP may be approved as set forth below:

1. *UDP That May Be Approved by the Assistant Commandant or a Delegee*. The Assistant Commandant for Intelligence (CG-2) or a delegee may approve the following types of UDP:

   a. **Education or Training**. Attending a course, meeting, seminar, conference, exhibition, trade fair, workshop, or symposium, or participating in educational or professional organizations, for the sole purpose of obtaining training or enhancing professional skills, knowledge, or capabilities of Coast Guard NIE personnel. Directing or tasking employees to conduct intelligence activities is not authorized under this category of UDP.

   b. **Cover Activities**. Participation in an organization solely for the purpose of maintaining or enhancing cover. Such participation may involve obtaining or renewing membership status or other activities and, in all cases, must be conducted in accordance with applicable cover policy. If the participation is not solely for the purpose of maintaining or enhancing cover or involves directing or tasking a person acting on behalf of the Coast Guard NIE to collect FI or CI from or about the organization or its members, the participation requires approval in accordance with other provisions of this paragraph or with Paragraphs F.2. or F.3.

   c. **Published or Posted Information.** Participation in an organization whose membership is open to the public solely for the purpose of obtaining information published or posted by the organization or its members and generally available to members. The method of obtaining this information must not involve elicitation.

   d. **Public Forums**. Participation in meetings, seminars, conferences, exhibitions, trade fairs, workshops, symposiums, or similar events sponsored or conducted by an organization, in person or through technical means (e.g., social networking sites, websites, or forums), provided that both of the following conditions are met:

      1) The activity is open to the public; and

      2) Participation is for the purpose of collecting CI or significant FI that is not focused on a specific U.S. person.

   e. **Foreign Entity.** Participation in an organization that is an entity openly acknowledged by a foreign government to be directed or operated by that foreign government or reasonably believed to be acting on behalf of a foreign power, and the organization is reasonably believed to consist primarily of individuals who are non-U.S. persons.

   f. **Non-U.S. Persons as Sources of Assistance**. To collect information necessary to identify and assess a non-U.S. person as a potential source of assistance to FI or CI activities.

   g. **U.S. Person Organizations outside the United States**. Participation in organizations outside the United States that constitute U.S. persons, to collect FI or CI outside the United States from or about a non-U.S. person located outside the United States.

2. *UDP That May Be Approved by Assistant Commandant for Intelligence (CG-2) or a Single Delegee*. The Assistant Commandant for Intelligence (CG-2) or a single delegee may approve the following types of UDP:

a. To collect FI outside the United States from or about a specific U.S. person or from or about a specific non-U.S. person in the United States.

b. To conduct authorized CI activities not addressed in Paragraph F.1. in or outside the United States, after required coordination with the FBI or CIA.

c. To collect information inside the United States necessary to identify a U.S. person as a potential source of assistance to FI or CI activities.

d. To collect information outside the United States necessary to assess a U.S. person as a potential source of assistance to FI or CI activities.

3. *Other UDP Approvals*. UDP that is not specifically addressed in this procedure may be authorized by the Assistant Commandant for Intelligence (CG-2) with notice to TJAG.

4. *Standards for Review and Approval*. The official approving the UDP pursuant to Paragraphs F.1., 2. or 3. must make all of the following determinations:

a. The potential benefits to national security from the UDP outweigh any adverse impact on civil liberties or privacy of U.S. persons. A factor in this determination will be whether the Coast Guard NIE will use appropriate safeguards, including limits on duration and scope of the UDP;

b. The proposed UDP complies with the limitations of Paragraph E.; and

c. The proposed UDP is the least intrusive means feasible and conforms to the requirements of Procedure 2.

G. Disclosure Requirement.

1. *General*. Unless the UDP is conducted in accordance with Paragraphs E. and F., disclosure of the intelligence affiliation of the person who is acting on behalf of the Coast Guard NIE will be made to an executive officer of the organization in question, or to an official in charge of membership, attendance, or the records of the organization. Such disclosure must be sufficient to apprise the official of the fact of the person's affiliation with the Coast Guard NIE (e.g., by identifying a Coast Guard unit with "Intelligence" in the title, or by stating the fact of intelligence affiliation where the name does not reveal the underlying affiliation).

2. *Serving as an Official of the Organization*. If the official to whom disclosure would be made is also acting on behalf of the Coast Guard NIE, his or her knowledge alone does not meet the disclosure requirement unless that person is the most senior official within the organization. Where the person is not the most senior official in the organization, disclosure must be made to an additional official with actual or apparent authority to act on behalf of the organization who is not affiliated with the IC in order for the participation not to be UDP.

3. *Records*. The Coast Guard NIE will maintain a written record of any disclosure of intelligence affiliation required by this procedure, including the name and title of the person to whom the disclosure was made.

ACRONYM LIST

CC	Chief Counsel
CI	Counterintelligence
CIA	Central Intelligence Agency
CGC	Coast Guard Commandant
CG-2	Assistant Commandant for Intelligence
CG-2d	Deputy Assistant Commandant for Intelligence
CG-LII	Chief, Information and Intelligence Law
CGCIS	Coast Guard Counterintelligence Service
DHS	Department of Homeland Security
DHS OGC	Department of Homeland Security Office of General Counsel
DIA	Defense Intelligence Agency
DIRNSA/CHCSS	Director, National Security Agency/Chief, Central Security Service
DNI	Director of National Intelligence
DoD	Department of Defense
DoDM	Department of Defense Manual
E.O.	Executive Order
FBI	Federal Bureau of Investigation
FI	Foreign Intelligence
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
IC	Intelligence Community
ICD	Intelligence Community Directive
IOO	Intelligence Oversight Official
LEI	Law Enforcement Intelligence
LEIE	Law Enforcement Intelligence Element
NIE	National Intelligence Element
NGA	National Geospatial-Intelligence Agency
NRO	National Reconnaissance Office
NSA/CSS	National Security Agency/Central Security Service
NSA OGC	National Security Agency Office of General Counsel
OGC	Office of General Counsel
ODNI	Office of the Director of National Intelligence
SIGINT	Signals Intelligence
IOO	Senior Intelligence Oversight Official
SOFA	Status of Forces Agreement
SLTT	State, local, tribal, or territorial
TJAG	The Judge Advocate General
TSCM	technical surveillance countermeasures
UDP	undisclosed participation
U.S.C.	United States Code

USPI	U.S. person information
USPS	United States Postal Service
USSS	United States SIGINT System
VCG	Vice Commandant Coast Guard

GLOSSARY - DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purpose of this Appendix.

Administrative purposes	Information that is received or collected when it is necessary for the administration of the Coast Guard NIE, but is not received or collected directly for intelligence purposes. Examples include information about systems administration; the performance of contractors; public affairs and legislative matters, including correspondence files; personnel and training records; and training materials.
Agent of a foreign power	Any person, including a U.S. person, who: 1. Knowingly engages in clandestine intelligence-gathering activities for, or on behalf of, a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States; 2. Pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for, or on behalf of, such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States; 3. Knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for, or on behalf of, a foreign power; 4. Knowingly enters the United States under a false or fraudulent identity for, or on behalf of, a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for, or on behalf of, a foreign power; or 5. Knowingly aids or abets any person in the conduct of activities described in Paragraphs (1) - (3) of this definition or knowingly conspires with any person to engage in such activities.
Coast Guard facilities	Installations or facilities owned, leased, or occupied by accommodation or otherwise by the Coast Guard.

Collection	Information is collected when it is received by the Coast Guard NIE, whether or not it is retained for intelligence or other purposes. Collected information includes information obtained or acquired by any means, including information that is volunteered to the NIE. Collected information does not include: • Information that only momentarily passes through a computer • system of the Coast Guard NIE; • Information on the internet or in an electronic forum or repository outside the Coast Guard NIE that is simply viewed or accessed by a Coast Guard employee but is not copied, saved, supplemented, or used in some manner; • Information disseminated to the Coast Guard NIE by other elements of the IC; or • Information that is maintained on behalf of another U.S. Government agency and to which the Coast Guard does not have access for intelligence purposes.
Communications Security (COMSEC)	A component of cybersecurity that deals with measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes cryptographic security, transmission security, emissions security, and physical security of COMSEC material. COMSEC does not include collecting FI or CI, or conducting any other intelligence activities.
Communications security investigation	An investigation, by an authorized investigative entity, conducted as a result of a COMSEC incident.
Concealed monitoring	The use of hidden electronic, optical, or mechanical devices to monitor a particular person or a group of persons without their consent in a surreptitious manner over a period of time, in circumstances in which such person or persons does not have a reasonable expectation of privacy. Monitoring is surreptitious when it is conducted in a manner designed to keep the subject of the monitoring unaware of it. Video monitoring or sound recording of a subject in a place where he or she has no reasonable expectation of privacy qualifies as concealed monitoring if conducted over a period of time, but taking one photograph of a subject would not qualify. Concealed monitoring does not include any monitoring or activities that constitute electronic surveillance (including as defined in FISA), physical searches, physical surveillance, overhead reconnaissance, or airborne reconnaissance.

Consent	An agreement by a person or organization to permit the Coast Guard NIE to take particular actions that affect that person or organization. Consent should be in written or in electronic form, but may be given orally, unless a specific form of consent is required by law or a particular procedure. Consent may be implied if legally adequate notice is provided or if an adequate policy has been published or otherwise articulated. The assigned legal counsel of the Coast Guard NIE will determine whether a notice or policy is adequate and lawful before the Coast Guard NIE relies on implied consent to take or refrain from taking an action.
Cooperating sources	Persons or organizations who knowingly and voluntarily provide information, or access to information, at the request of the Coast Guard NIE, or on their own initiative. "Cooperating sources" may include government agencies, law enforcement authorities, credit agencies, academic institutions, businesses, employers, private citizens, and foreign governments.
Counterintelligence (CI)	Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.
Detail	A status under which, by agreement between government agencies or elements of the IC, an employee of one agency or element operates under the authorities, regulations, policies, and supervision of another.
Dissemination	The transmission, communication, sharing, or passing of information outside the Coast Guard NIE by any means, including oral, electronic, or physical means. Dissemination includes providing any access to information in the Coast Guard NIE's custody to persons outside the Coast Guard NIE.
Domestic activities	Activities that take place within the United States that do not have a significant connection with either an agent of a foreign power or a foreign power, organization, or person.

Electronic surveillance	Acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a non-electronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter. Electronic surveillance is also defined in FISA, and where this Appendix references that definition, FISA should be consulted.
Foreign connection	As applied to a U.S. person, a reasonable belief that the U.S. person is or has been in contact with, or has attempted to contact, a foreign person or a representative or agent of a foreign country, for purposes harmful to the national security interests of the United States; or a reasonable belief that the U.S. person is acting or encouraging others to act in furtherance of the goals or objectives of a foreign person or power, or a representative or agent of a foreign power, for purposes harmful to the national security interests of the United States.
Foreign Intelligence (FI)	Information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists.
Foreign power	Any of the following: • A foreign government or any component thereof, whether or not recognized by the United States. • A faction of a foreign nation or nations, not substantially composed of U.S. persons. • An entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments. • A group engaged in international terrorism or activities in preparation therefor. • A foreign-based political organization, not substantially composed of U.S. persons. • An entity that is directed and controlled by a foreign government or governments. • An entity not substantially composed of U.S. persons that is engaged in the international proliferation of weapons of mass destruction.

Host of a shared repository	An entity responsible for developing and maintaining a shared repository. A host may or may not have access to information in the repository for intelligence purposes.
Imagery	A likeness or presentation of any natural or manmade feature or related object or activity and the positional data acquired at the same time the likeness or representation was acquired, including products produced by space-based national intelligence reconnaissance systems and likenesses or presentations produced by satellites, airborne platforms, unmanned aerial vehicles, or other similar means. Imagery does not include handheld or clandestine photography taken by or on behalf of human intelligence collection organizations. This definition is consistent with Section 467 of Title 10, U.S.C.
Incidental collection of USPI	Collection of USPI that is not deliberately sought by the Coast Guard NIE, but that is nonetheless collected. Collection of USPI that is not deliberately sought is considered incidental regardless of whether it is expected or reasonably anticipated to occur.
Intelligence	Includes foreign intelligence (FI) and counterintelligence (CI).
Intelligence activities	As applied to the NIE, activities undertaken by Coast Guard NIE personnel pursuant to E.O. 12333.
Intelligence Community (IC) and elements of the Intelligence Community	• The ODNI. • The CIA. • The National Security Agency/Central Security Service (NSA/CSS). • The Defense Intelligence Agency (DIA). • The NGA. • The National Reconnaissance Office (NRO). • The intelligence and counterintelligence elements of the Army, the Navy, the Air Force, and the Marine Corps. • The intelligence elements of the FBI. • The Office of National Security Intelligence of the Drug Enforcement Administration. • The Office of Intelligence and Counterintelligence of the Department of Energy. • The Bureau of Intelligence and Research of the Department of State.

	• The Office of Intelligence and Analysis of the Department of the Treasury. • The Office of Intelligence and Analysis of DHS. • The intelligence and counterintelligence elements of the Coast Guard. • The other offices within DoD for the collection of specialized national foreign intelligence through reconnaissance programs. • Such other elements of any other department or agency as may be designated by the President, or designated jointly by the DNI and the head of the department or agency concerned, as an element of the IC.
Intentional collection of USPI	Collection of USPI that is deliberately sought by the Coast Guard NIE.
International narcotics activities	Activities outside the United States involving the production, transfer, or sale of significant quantities of narcotics or other substances controlled in accordance with Sections 811 and 812 of Title 21, U.S.C., or activities inside the United States that are directly tied to such activities outside the United States.
International terrorism or international terrorist activities	Activities that involve violent acts or acts dangerous to human life that violate federal, state, local, or tribal criminal law or would violate such law if committed within the United States or a State, local, or tribal jurisdiction; appear to be intended to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, or affect the conduct of a government by assassination or kidnapping; and occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear to be intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.
Mail cover	The nonconsensual recording of any data appearing on the outside cover of any sealed or unsealed mail matter. In this context, a "recording" means a transcription, photograph, photocopy, or other facsimile of the image or information on the outside cover, envelope, or wrappers of mail matter. A mail cover does not include any opening or examination of mail that constitutes a physical search.

Mail in USPS channels	Mail while in transit within, among, and between the United States (including mail of foreign origin that is passed by a foreign postal administration to the U.S. Postal Service (USPS) for forwarding to a foreign postal administration under a postal treaty or convention and mail temporarily in the hands of the U.S. Customs Service or the Department of Agriculture), mail to or from the Military Postal Service Agency, Army or Air Force Post Offices and Fleet Post Offices, and mail for delivery to the United Nations, New York. Mail in USPS channels includes international mail in transit to an addressee in the United States after receipt by the USPS from a foreign postal administration or international mail in transit to an addressee abroad before passage to a foreign postal administration. Mail is in transit until it is physically delivered to the specific addressee in the United States who is named on the envelope or his or her authorized agent.
National Intelligence Element (NIE)	The Coast Guard NIE consists of only those intelligence elements and persons designated by the Assistant Commandant for Intelligence (CG-2) and which are subject to the National Security Act of 1947, E.O. 12333, and other authorities applicable to the Intelligence Community as defined in the National Security Act of 1947.
NIE personnel	Those personnel employed by, assigned or detailed to, or acting for the Coast Guard NIE, acting under the authority, direction, and control of the Coast Guard NIE, or designated by the Assistant Commandant for Intelligence (CG-2) as part of the Coast Guard NIE. This includes government employees, contract employees, individuals working for a contractor, Coast Guard military personnel, or other persons or entities providing services to or acting on behalf of the Coast Guard NIE for intelligence purposes. This term does not include a cooperating source.

Organization	For purposes of Procedure 10, and for purposes of the definitions of "organization in the United States," "organization outside the United States," "organization outside the United States that constitutes a U.S. person," "participation in an organization," and "undisclosed participation," an organization is an association of two or more individuals formed for any lawful purpose whose existence is formalized in some manner (e.g., by having a defined leadership, holding meetings, publishing a charter, or requiring dues). The term "organization" includes corporations, other commercial entities, and associations formed for a social, political, fraternal, professional, business, academic, ethnic-affinity, or religious purpose, including those that meet and communicate through the use of technologies. The term "organization" does not include a loose group of friends, social contacts, or business associates who may share common interests but whose association lacks any formal structure. For example, the Rotary Club is an organization; a group of friends who play poker or meet at a gym for athletics every weekend is not. NIE personnel should consult with the appropriate legal office if there is any question as to whether a group or an entity constitutes an organization.
Organization in the United States	An organization physically located in the United States, whether or not it constitutes a U.S. person. Thus, a branch, subsidiary, or office of an organization in the United States that is physically located outside the United States is not an organization in the United States. Conversely, a branch, subsidiary, or office of a foreign organization, or one substantially made up of foreign persons that are physically located in the United States is an organization in the United States. An organization in the United States includes an organization that primarily meets and communicates on the internet or through the use of other technologies and is substantially composed of persons who are located in the United States.
Organization outside the United States that constitutes a U.S. person	An organization physically located outside the United States that is substantially composed of U.S. persons. This definition includes an organization that primarily meets and communicates on the internet or through the use of other technologies and is substantially composed of U.S. person who are located outside the United States.
Overhead reconnaissance	Activities carried out by space-based capabilities whose principal purpose is conducting or enabling imagery collection.

Participation in an organization	Taking part in an organization's activities or interacting with its members within the structure or framework of the organization. Such activities may include one or more of the following: acquiring membership; attending or taking part in meetings, events, activities, or other forums sponsored or conducted by the organization; conducting the work or functions of the organization; serving as a representative or agent of the organization; or contributing funds to the organization other than in payment for goods or services. Actions taken outside the organizational structure or framework, however, do not constitute participation. Thus, attendance at meetings or social gatherings that involve the organization's members, but are not functions or activities of the organization itself, does not constitute participation. Participation is "on behalf of" the Coast Guard NIE when a person is tasked or asked to participate in an organization for the benefit of the Coast Guard NIE. Such a person may already be a member of the organization or may be asked to join. Actions undertaken for the benefit of the Coast Guard NIE may include collecting information, identifying potential sources or contacts, or establishing or maintaining cover. Participation "for the purpose of influencing the activities of an organization or its members" is any action taken with the intention of causing a significant effect on the organization's agenda, course of business, core activities, or future direction. Simply voting or expressing an opinion on these matters as a member generally will not fall within this definition. NIE personnel should consult with the legal office responsible for advising their element or office if there is any question as to whether an activity constitutes participation.
Personnel security	The security discipline that assesses the loyalty, reliability, and trustworthiness of individuals for initial and continued eligibility for access to classified information or assignment in sensitive positions.

Personnel security investigation	Any investigation required for the purpose of determining the eligibility of Coast Guard military or civilian personnel, contractor employees, consultants, or other persons affiliated with the Coast Guard for access to classified information, acceptance or retention in the military services, assignment or retention in sensitive positions, or assignment of other designated duties requiring such investigation. It also includes investigations of allegations that arise subsequent to adjudicative action and require resolution to determine an individual's current eligibility for a national security position.
Physical search	Any intrusion on a person or a person's property or possessions for the purpose of obtaining property, information, or stored electronic data or communications that would require a warrant for law enforcement purposes. A physical search includes an intrusion that violates a reasonable expectation of privacy or that involves a trespass, or otherwise physically occupying a constitutionally protected area, to obtain information. It also includes the examination of the interior of property, or the scan of a person, by technical means. A physical search generally does not include: • Examinations of areas that are in plain view and visible to the unaided eye if there is no physical trespass; • Examinations of publicly available information; • Examinations of abandoned property in a public place; • Examinations of government property pursuant to Military Rule of Evidence 314(d), Manual for Courts-Martial; • Electronic surveillance (including as defined in FISA); or • Any intrusion authorized as needed to accomplish lawful electronic surveillance as that term is defined in FISA, conducted in accordance with Procedure 5. The law in this area is subject to change, and NIE personnel should consult with the appropriate legal office on those activities that may constitute a physical search.

Physical surveillance	The deliberate and continuous observation of a person to track his or her movement or other physical activities while they are occurring, under circumstances in which the person has no reasonable expectation of privacy. An employee of CGCIS may operate enhancement devices (*e.g.*, binoculars or still or full motion cameras) to facilitate a physical surveillance. Physical surveillance does not include casual observation that is short in duration and not intended to track the movement or other physical activities of a person; nor does it include any activity that constitutes electronic surveillance (including as defined in FISA), a physical search, or overhead reconnaissance.
Publicly available information	Information that has been published or broadcast for public consumption, is available on request to the public, is accessible on-line or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public. Publicly available information includes information generally available to persons in a military community even though the military community is not open to the civilian general public.
Radio communications hearability survey	The monitoring of radio communications to determine whether a particular radio signal can be received at one or more locations and, if reception is possible, to determine the hearability of reception over time.
Reasonable belief	When the facts and circumstances are such that a reasonable person would hold the belief. A reasonable belief must rest on facts and circumstances that can be articulated; hunches or intuitions are not sufficient. A reasonable belief can be based on experience, training, and knowledge of FI or CI activities as applied to particular facts and circumstances, and a trained and experienced person might hold a reasonable belief that is sufficient to satisfy these criteria when someone unfamiliar with FI or CI activities might not.
Reasonable expectation of privacy	An expectation that a person has, and that society is prepared to recognize as reasonable under the facts and circumstances presented, that his or her person, location or activities, property, possessions, or communications are private from the government. Whether a person's expectations are reasonable is fact-specific, and the law in this area is subject to change. TJAG or a servicing legal office should determine whether a person has a reasonable

	expectation of privacy.
Retention	The maintenance of information in either hard copy or electronic format regardless of how the information was collected or how it was disseminated by another IC element.
Senior Intelligence Oversight Official (SIOO)	The Coast Guard official designated as the most senior person responsible for intelligence oversight. Normally this will be TJAG, also known as the Coast Guard Chief Counsel (CC).
Shared repository	A database, environment, or other repository maintained for the use of more than one entity. A database, environment, or other repository that a contractor or other entity maintains for the use of a single entity, or those acting on its behalf, is not a shared repository.
Technical surveillance countermeasures (TSCM)	The use of electronic surveillance equipment, other electronic or mechanical devices, or specialized techniques and measures to determine either the existence and capabilities of unauthorized, hostile, or foreign penetration technologies that are used to obtain unauthorized access to classified or sensitive information, and thereby assist in neutralizing and exploiting such technologies, or the susceptibility of electronic equipment to unlawful electronic surveillance.
The Judge Advocate General (TJAG)	The senior attorney in the Coast Guard, designated by DHS General Counsel as the Judge Advocate General. TJAG is also the Coast Guard Chief Counsel (CC), and serves as the SIOO.
Transmission media vulnerability survey	The acquisition of radio frequency propagation and its subsequent analysis to determine empirically the vulnerability of the transmission media to interception by foreign intelligence services.
Undisclosed participation (UDP)	Participation in any organization in the United States, or any organization outside the United States that is a U.S. person, if the person's intelligence affiliation is not disclosed to an appropriate official of the organization.
United States	When used in the geographic sense, the land area, internal waters, territorial seas, and airspace of the United States, to include U.S. territories, possessions, and commonwealths.

U.S. person	Includes: • A U.S. citizen. • An alien known by the Coast Guard NIE to be a permanent resident alien. • An unincorporated association substantially composed of U.S. citizens or permanent resident aliens. • A corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. A corporation or corporate subsidiary incorporated abroad, even if partially or wholly owned by a corporation incorporated in the United States, is not a U.S. person. A person or organization in the United States is presumed to be a U.S. person, unless specific information to the contrary is obtained. Conversely, a person or organization outside the United States, or whose location is not known to be in the United States, is presumed to be a non-U.S. person, unless specific information to the contrary is obtained.
U.S. person information (USPI)	Information that is reasonably likely to identify one or more specific U.S. persons. USPI may be either a single item of information or information that, when combined with other information, is reasonably likely to identify one or more specific U.S. persons. Determining whether information is reasonably likely to identify one or more specific U.S. persons in a particular context may require a case-by-case assessment by a trained intelligence professional. USPI is not limited to any single category of information or technology. Depending on the context, examples of USPI may include: names or unique titles; government-associated personal or corporate identification numbers; unique biometric records; financial information; and street address, telephone number, and internet protocol address information. USPI does not include: • A reference to a product by brand or manufacturer's name or the use of a name in a descriptive sense, as, for example, Ford Mustang or Boeing 737; or • Imagery from overhead reconnaissance, or information about conveyances (e.g., vehicles, aircraft, or vessels), without linkage to additional identifying information that ties the information to a specific U.S. person.

SIGNATURE PAGE

We approve the foregoing Procedures in accordance with Executive Order 12333, as amended.

Karl L. Schultz, Admiral
Commandant
U.S. Coast Guard

24 NOVEMBER 2020
Date

William P. Barr
Attorney General

December 23, 2020
Date

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B – ADDITIONAL COAST GUARD POLICY FOR CONDUCTING NATIONAL INTELLIGENCE ELEMENT (NIE) ACTIVITIES

A. Introduction.

This Appendix provides guidance on the conduct of foreign intelligence (FI) and counterintelligence (CI) activities by the Coast Guard National Intelligence Element (NIE). It identifies circumstances where approval is required for Coast Guard conduct of certain FI and CI activities as required by Executive Order (E.O.) 12333.

B. Procedures.

The procedures set forth in this Appendix apply only to National Intelligence Element (NIE) personnel when they are conducting FI and CI activities. Coast Guard personnel detailed to another Intelligence Community (IC) organization must comply with the E.O. 12333 implementing procedures of that organization rather than this Manual.

PROCEDURE 11 – CONTRACTING FOR GOODS AND SERVICES

A. Applicability.

1. This Procedure applies to contracting and other arrangements with U.S. persons for the procurement of goods and services by the NIE within the United States and with contractors not within the United States who are U.S. persons. It does not apply to contracting with government entities or to the enrollment of NIE personnel in academic institutions (covered under Procedure 10).
2. For the purpose of this procedure, NIE personnel enter into contracts "for the procurement of goods and services" when the contract is entered into on behalf of the NIE. The Coast Guard Law Enforcement Intelligence Element (LEIE) will not be used to enter into contracts on behalf of the NIE to circumvent this procedure.

B. Definition of Terms.

See the Glossary for definitions of "academic institution," "National Intelligence Element (NIE)," "NIE Personnel," "United States," and "U.S. person."

C. Procedures.

1. The NIE is authorized to enter into contracts for the procurement of goods and services with an academic institution as long as prior to the making of the contract, the Coast Guard has disclosed to appropriate officials of the academic institution the fact of the sponsorship or involvement by the NIE.
2. The NIE is authorized to enter into contracts for the procurement of goods and services with commercial organizations, private institutions, or private individuals within the United States without revealing sponsorship or involvement of the NIE if:
   a. The contract is for published material available to the general public or for routine goods or services necessary for the support of approved activities, such as credit cards, car rentals, travel, lodging, meals, rental of office space, and other items incidental to approved activities; or
   b. There is a written determination by the Assistant Commandant for Intelligence (CG-2), with concurrence from The Judge Advocate General (TJAG), that the sponsorship or involvement of the NIE must be concealed to protect the activities of the NIE concerned.

D. Effect of Non-Compliance.

No contract must be void or voidable for failure to comply with this procedure.

PROCEDURE 12 – PROVISIONS OF ASSISTANCE TO LAW ENFORCEMENT ORGANIZATIONS, REGULATORY AGENCIES AND OTHER CIVIL AUTHORITIES

A. Applicability.

This Procedure applies to the provision of assistance by the NIE to law enforcement organizations, regulatory agencies, and other civil authorities.

B. Definition of Terms.

See the Glossary for definitions of the "alien," "civil authorities," "NIE," "organizations," "regulatory agencies,", and "United States."

C. Procedures.

The NIE is authorized to cooperate with law enforcement organizations, regulatory agencies, and other civil authorities for the purpose of:

1. Investigating, preventing, or mitigating:
    a. Intelligence activities of foreign intelligence entities or powers,
    b. International narcotics activities,
    c. International terrorist activities,
    d. International maritime alien migration,
    e. International fisheries threats, and
    f. International environmental threats.
2. Provide assistance to:
    a. Search and rescue,
    b. Marine safety,
    c. Aids to navigation,
    d. International ice breaking operations,
    e. Department of Homeland Security (DHS) emergency response operations, and
    f. Render any other assistance and cooperation allowed by law.
3. Protecting Coast Guard employees, information, property and facilities; and
4. Preventing, detecting, or investigating other violations of law.

D. Types of Permissible Assistance.

The NIE is authorized to provide the following types of assistance to law enforcement organizations, regulatory agencies, and other civil authorities:

a. *Information.* Information disseminated by the NIE must be disseminated in accordance with Appendix A, Procedure 4 and applicable policies implementing E.O. 13526 on "Classified National Security Information" and E.O. 13549 on "Classified National Security Information Program for State, Local, Tribal, and Private Sector (SLTPS) Entities," and the Coast Guard Intelligence Manual, COMDTINST 3800.6 (series). All information must be disseminated in a manner that protects intelligence sources and methods.

   1) Information reasonably believed to indicate a violation of federal law must be disseminated to other federal agencies through the Coast Guard Investigative Service (CGIS).

   2) Information reasonably believed to indicate a violation of state, local, or foreign laws may be disseminated in accordance with the policy and procedures authorized in the Coast Guard Intelligence Manual, COMDTINST 3800.6 (series).

b. *Equipment, Facilities, Technical Knowledge and Expert Personnel.* Specialized equipment and facilities, technical knowledge, or the assistance of expert personnel may be provided to federal law enforcement agencies, regulatory agencies, and other civil authorities, and, when lives are endangered, to state and local government organizations, provided that such assistance has been approved by Commandant (CG-2), or a designated delegee, and in the case of expert personnel by Commandant (CG-2) and TJAG or delegee. Specialized equipment or facilities that are associated with the United States SIGINT System (USSS) cannot be provided without the approval of the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS) or a designated representative.

   1) *Personnel.* NIE personnel may be assigned by appropriate Command authority to support law enforcement activities insofar as they do not use NIE resources, funding, equipment, or authorities. Use of NIE resources, funding, equipment, or authorities in support of law enforcement activities, including direct participation in law enforcement activities (e.g., boardings, search, seizure, and arrest) require approval by Commandant (CG-2) or delegee, with concurrence of TJAG or delegee. To ensure compliance with Procedure 12, NIE components seeking to assign NIE personnel to support activities other than NIE missions first must consult with their servicing legal counsel to ascertain whether Commandant (CG-2) or delegee approval is required to detail said personnel and to ensure that all NIE personnel are appropriately trained before said personnel are detailed. Servicing legal counsel will consult with Chief, CG-LII, before determining that a situation does not require Commandant (CG-2)/TJAG approval under this procedure.

E. Administration of Military Justice.

Procedure 12 does not prohibit the NIE from administering military justice over NIE members as authorized by the Uniform Code of Military Justice (UCMJ), Manual for Courts-Martial-United States, and Military Justice Manual, COMDTINST M5810.1 (series), in maintaining good order and discipline.

F. Assistance to the Federal Bureau of Investigation (FBI) National Security and Foreign Intelligence Investigative Activities.

The NIE is authorized to conduct FI and CI activities to assist the FBI during national security or FI/CI investigative activities, as appropriate. Providing intelligence assistance to the FBI for national security related matters or FI and CI investigative activities is generally not considered "assistance to law enforcement" under this Procedure. All counterintelligence assistance provided to the FBI must be coordinated with the Director, Coast Guard Counterintelligence Service (CGCIS), or a designated representative.

PROCEDURE 13 – EXPERIMENTATION ON HUMAN SUBJECTS

A. Applicability.

This procedure applies to the experimentation on human subjects when an experiment is conducted by or on behalf of the NIE.

1. "Experimentation" means any research or testing activity involving human subjects that may expose the subjects to the possibility of permanent or temporary injury (including both physical and psychological injury) beyond the risk of injury to which the subjects are ordinarily exposed.
2. Experimentation is conducted on behalf of the NIE whenever an experiment is conducted under contract to the NIE, for the benefit of the NIE, or at the request of the NIE, regardless of any contractual relationship.

B. Definition of Terms.

See the Glossary for definitions of "CI", FI", "human subjects", "NIE," "physical injury", and "psychological injury".

C. Procedures.

Experimentation on human subjects by the NIE for FI or CI purposes is strictly prohibited.

PROCEDURE 14 – EMPLOYEE CONDUCT

A. Applicability.

This Procedure sets forth the responsibilities of Commandant (CG-2), and supervisors and personnel of the NIE to conduct themselves in accordance with E.O. 12333 and the provisions of this Manual.

B. Definition of Terms.

See the Glossary for definitions of "NIE," "person," "physical injury," "U.S. Person," and "Whistleblower Protection."

C. Procedures.

1. The NIE must conduct intelligence activities only in accordance with E.O. 12333, the provisions of this Manual, and other applicable laws, Executive Orders, regulations, and Coast Guard Instructions with due diligence to protect the civil rights and civil liberties of U.S. persons and all others entitled to such protections.
2. Commandant (CG-2) and supervisors of the NIE must ensure that NIE personnel are thoroughly familiar with E.O. 12333 and the provisions of this Manual, and are regularly trained and exercised in the application of those rules to the conduct of intelligence activities. Particular emphasis must be placed on Appendix A. Procedures 1-4 and Procedures 12, 14, and 15 found in this Appendix.
3. Commandant (CG-2), supervisors of the NIE, and its personnel must:
    a. Ensure that all planned or conducted intelligence activities that may be unlawful are reported in accordance with Procedure 15;
    b. In accordance with the IC's Whistleblower Protection Policy (ICD 120), ensure that no adverse action is taken against any person because that person reports activities pursuant to Procedure 15;
    c. Impose appropriate corrective, administrative, or disciplinary action on NIE personnel who violate the provisions of this Manual, laws, executive orders, Presidential directives, or other applicable directives governing the conduct of intelligence activities; and
    d. Ensure that TJAG, individuals designated to conduct oversight inspections (e.g., Office of Information and Intelligence Law (CG-LII)), the Inspector General and General Counsel of the DHS, Office of the Director of National Intelligence (ODNI) Inspector General, and the Intelligence Oversight Board (IOB) have access to any information necessary to perform their duties assigned by statute, executive order, or the provisions of this Manual.

PROCEDURE 15 – IDENTIFYING, INVESTIGATING, AND REPORTING QUESTIONABLE INTELLIGENCE ACTIVITIES AND CONDUCT OF OVERSIGHT FUNCTIONS

A. Applicability.

This Procedure provides for the identification, investigation, and reporting of questionable intelligence activities (QIAs) and significant or highly sensitive matters (S/HSM).

B. Definition of Terms.

See the Glossary for definitions of "CI," FI," "IOO," NIE Personnel," "NIE," "OGC," "person," "QIAs," "U.S. Person," "S/HSM," and "Whistleblower Protection."

C. Procedures Governing QIAs and S/HSMs.

1. *Identification.*

   a. NIE personnel must immediately report any QIA or S/HSM to their chain of command or Intelligence Oversight Official (IOO) by the most rapid means. If it is not practical to report a QIA or S/HSM to the chain of command or IOO, reports may be made to Commandant (CG-LII), TJAG, the DHS Office of the General Counsel (OGC); DHS Office of Inspector General (IG); or the IC IG.

   b. IOOs and supervisors of the NIE who receive a report of a QIA or S/HSM must immediately notify Commandant (CG-LII), who must advise Commandant (CG-2) and TJAG.

2. *Investigation.*

   a. Each report of a QIA or S/HSM will be investigated to the extent necessary to determine the facts and to assess whether the activity is legal and consistent with applicable policies. At a minimum, investigations will require a written report that includes a description of the incident and a determination of whether the allegation was substantiated. Investigations will be conducted in accordance with the Coast Guard Administrative Investigation Manual, COMDTINST M5830.1 (series) or a manner otherwise prescribed by Commandant (CG-2). If the allegation is substantiated, the report will include findings of fact, an assessment of the cause, and recommended remedial action to prevent recurrence.

   b. All QIAs and S/HSMs will be referred to TJAG, through Commandant (CG- LII), for review and action under an appropriate authority. If Commandant (CG-LII) determines that the activity may constitute a crime or indicate a person may be acting for or on behalf of a foreign intelligence entity, the activity must also be properly reported to Director, CGCIS; Director, CGIS; or the FBI, in accordance with Coast Guard policy.

      i. If the QIA or S/HSM involves possible violations of federal criminal law or actions by employees assigned to the NIE or intelligence activities that may be

unlawful or contrary to Executive Order or Presidential Directive, the servicing legal office must notify TJAG, through Commandant (CG-LII) for further action under Procedure 15, Paragraphs C. and D.

ii. If the QIA does not involve matters specified in Procedure 15, Paragraphs C. and D., Commandant (CG-LII) must forward the report to the supervisor of the NIE employee concerned for appropriate action.

c. Nothing in this Manual can interfere with the authority and function of the IG with respect to criminal investigations of civilian employees, investigations, inspections, and audits of Coast Guard activities, or intelligence oversight responsibilities assigned to the DHS IG under E.O. 13462.

3. Reporting.

a. TJAG Reporting Parameters.

i. TJAG will report the following matters to the DHS OGC:

1) QIAs.

2) S/HSMs.

3) Any intelligence or intelligence-related activity that has been or will be reported to the U.S. Attorney General, or that must be reported to the U.S. Attorney General as required by law or other directive, including crimes required by E.O. 12333 to be reported to the U.S. Attorney General.

ii. TJAG will notify DHS OGC before providing briefings to any congressional committee, member of Congress, or congressional staff concerning intelligence or intelligence-related matters that meet the reporting criteria for QIAs, S/HSMs, or crimes reported to the U.S. Attorney General, unless extenuating circumstances exist. Should extenuating circumstances prevent advance notification to the DHS OGC, then he or she will be updated on the briefing's outcome as soon as possible.

b. TJAG Reporting Timelines.

i. All S/HSMs must be immediately forwarded to DHS OGC. Such reports may be made by any secure means. Oral reports will be documented with a written report as soon as possible thereafter. Initial reports will be supplemented as additional information becomes available. Supplemental reports will be identified in such a manner that they can be accurately related to the relevant initial reports.

ii. QIAs Quarterly to the DHS OGC. Quarterly reporting periods are based on the calendar year. The first report for each calendar year will cover January 1 through March 31. Succeeding reports will follow at 3-month intervals. Quarterly reports are due to DHS OGC by the 15th day of the month following the end of the quarter, unless other arrangements have been approved by the

DHS OGC. Quarterly reports will describe all QIAs, S/HSMs, and crimes required by E.O. 12333 to be reported to the U.S. Attorney General that were identified during the quarter. Quarterly reports are required even if no QIA or S/HSM occurred during the reporting period.

c. Reporting Format.

i. Reporting format will be conducted in accordance with Oversight of Coast Guard Intelligence Activities, COMDTINST 3821.12 (series).

D. Procedures Governing Violations of Criminal Laws.

This Section implements § 1.6 (a) of E.O. 12333 regarding reporting of possible commission of federal crimes by NIE personnel to the Attorney General, which requires TJAG to report possible violations of federal criminal law by employees assigned to the NIE to the DHS General Counsel and the Attorney General in accordance with procedures established by the Department of Justice (DoJ).

E. Congressional Notification (ICD 112).

Congressional notification is required, in writing-as appropriate, of all S/HSM (e.g., significant anticipated intelligence activities, significant intelligence failures, significant intelligence activities, and illegal activities). Commandant (CG-2), with concurrence by TJAG, is responsible for determining whether an event is reportable under ICD 112 and is responsible for ensuring that Congress is notified of all intelligence activities in accordance with the provisions of ICD 112.

F. Conduct of Oversight Inspections.

1. TJAG must ensure the conduct of regular inspections of the NIE to ensure compliance with applicable statutes, executive orders, and directives governing the conduct of FI and CI activities, and the provisions of this Manual. Such inspections must be conducted by employees designated by TJAG, such as the Intelligence Oversight Officials (IOO) assigned to the NIE (e.g., attorneys within Commandant (CG-LII), staff elements of the Commandant (CG-2), or other IC or DHS oversight officials). Oversight of Coast Guard Intelligence Activities, COMDTINST 3821.14 (series), provides further guidance on intelligence oversight inspections.
2. Procedure 15, Paragraph F. cannot interfere with oversight inspections conducted by other authorized entities, including the DHS IG, DHS OGC, IC IG, or the IOB.

ACRONYM LIST

CI	See Appendix A
DHS	See Appendix A
DIRNSA/CHCSS	See Appendix A
E.O.	See Appendix A
FI	See Appendix A
IC	See Appendix A
ICD	See Appendix A
IG	Inspector General
IOB	Intelligence Oversight Board
IOO	See Appendix A
LEIE	See Appendix A
NIE	See Appendix A
ODNI	See Appendix A
OGC	See Appendix A
QIA	Questionable Intelligence Activity
S/HSM	Significant or Highly Sensitive Matter
SLTPS	State, Local, Tribal, and Private Sector (DHS)
UCMJ	Uniform Code of Military Justice
USSS	See Appendix A
USPI	See Appendix A

GLOSSARY - DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purpose of this Appendix.

Academic Institution	Is an educational institution dedicated to education and research, which grants academic degrees. See also academy and university.
Alien	Any person who is not a citizen or a national of the United States.
Civil Authorities	Civil authority or civilian authority, also known as civilian government, is the practical implementation of a State, other than its military units, that enforces law and order. It is also used to distinguish between religious authority (for example Canon law) and secular authority.
Counterintelligence (CI)	See Appendix A Glossary.
Foreign Intelligence (FI)	See Appendix A Glossary.
Foreign power	See Appendix A Glossary
Human Subjects	Is defined as a living individual about whom an investigator conducting research obtains (1) data through intervention or interaction with the individual, or Identifiable private information about whom includes a subject's opinion on a given topic.
Intelligence	Includes Foreign Intelligence (FI) and Counterintelligence (CI).
Intelligence Activities	See Appendix A Glossary
Intelligence Community (IC) and elements	See Appendix A Glossary

Intelligence Oversight	The process of independently ensuring all foreign intelligence and counterintelligence activities are conducted in accordance with applicable United States law, executive orders, Presidential Directives, Intelligence Community, Department of Homeland Security (DHS), and Coast Guard policy instructions designed to balance the requirement for acquisition of essential information by the IC, and the protection of Constitutional and statutory rights of U.S. persons. Intelligence Oversight also includes the identification, investigation, and reporting of questionable intelligence activities.
Intelligence Oversight Official (IOO)	A Coast Guard employee designated by the TJAG to provide intelligence oversight guidance and advice to NIE component employees.
National Intelligence Element (NIE)	See Appendix A Glossary.
NIE Personnel	See Appendix A Glossary.
Organization	See Appendix A Glossary.
Permanent Resident Alien	Any person not a citizen of the United States who is living in the United States under legally recognized and lawfully recorded permanent residence as an immigrant.
Physical Injury	Is a legal term for an injury to the body, mind or emotions, as opposed to an injury to property.
Psychological Injury	Refers to psychological or psychiatric conditions associated with an event that leads, or may lead, to a lawsuit in tort action or other legal-related claims. Psychological injury is not just workplace stress, it is a stress response to the point of a psychological disorder. Examples of psychological injury are depression, post-traumatic stress disorder (PTSD), and anxiety disorders.
Questionable Intelligence Activities (QIA)	Any intelligence or intelligence-related activity when there is reason to believe such activity may be unlawful or contrary to an E.O., Presidential Directive, ICD, or applicable DoD or

	Coast Guard policy governing that activity.
Regulatory Agencies	A public authority or government agency responsible for exercising autonomous authority over some area of human activity in a regulatory or supervisory capacity. (aka regulatory authority, regulatory body or regulator)
Significant or Highly Sensitive Matters (S/HSM)	An intelligence or intelligence-related activity (regardless of whether the intelligence or intelligence-related activity is unlawful or contrary to an E.O., Presidential Directive, ICD, Coast Guard or other applicable policy), or serious criminal activity by intelligence personnel, that could impugn the reputation or the integrity of the IC, or otherwise call into question the propriety of intelligence activities. Such matters might involve actual or potential: • Congressional inquiries or investigations. • Adverse media coverage. • Impact on foreign relations or foreign partners. Systemic compromise, loss, or unauthorized disclosure of protected information. See Memorandum dtd 19 February 2010 from the Assistant Commandant for Intelligence and Criminal Investigations, SUBJ: Policy Update - Reports to Executive and Legislative Branches Re: Intelligence Oversight and Significant Activities for more information on S/HSMs.
United States	See Appendix A Glossary
United States Person (U.S. Person)	See Appendix A Glossary
Whistleblower Protection	A whistleblower is an employee that reports an employer's misconduct. There are laws that protect whistleblowers from being fired or mistreated for reporting misconduct. One of these laws is the Whistleblower Protection Act.

THIS PAGE INTENTIONALLY LEFT BLANK