U.S. Department of Homeland Security

United States Coast Guard

# Coast Guard Intelligence Oversight Manual

**COMDTINST M3821.14A**
**April 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 JR. Ave SE
Washington, DC 20593-7301
Staff Symbol: CG-094
Phone: (202) 372-2700

COMDTINST M3821.14A
12 APR 2021

COMMANDANT INSTRUCTION M3821.14A

Subj: COAST GUARD INTELLIGENCE OVERSIGHT

Ref:
(a) Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended
(b) Executive Order 13462, "President's Intelligence Advisory Board and Intelligence Oversight Board," February 29, 2008, as amended
(c) Executive Order 13286, "Amendment of Executive Orders, and Other Actions, in Connection With the Transfer of Certain Functions to the Secretary of Homeland Security," February 28, 2003
(d) Chairman, Intelligence Oversight Board memo of 27 May 2015, Subj: Intelligence Oversight Board's Concept of Operations
(e) Coast Guard Intelligence Activities, COMDTINST M3820.12 (series)
(f) Coast Guard Intelligence Manual (CGIM), COMDTINST M3800.6 (series)
(g) National Security Act of 1947, as amended (50 U.S.C. 3021 *et seq*.)
(h) Secretary of Homeland Security memo of 29 Sep 2008, Subj: Executive Order 13462: President's Intelligence Advisory Board and Intelligence Oversight Board Section 8(b)(ii)
(i) Intelligence Community Directive 112, Congressional Notification, 29 Jun 2017
(j) Assistant Commandant for Intelligence and Criminal Investigations memo of 19 Feb 2010, Subj: Policy Update – Reports to Executive and Legislative Branches Re: Intelligence Oversight and Significant Activities
(k) Intelligence Community Directive 120, Intelligence Community Whistleblower Protection, 29 April 2016
(l) Presidential Policy Directive (PPD)-19, Protecting Whistleblowers with Access to Classified Information, 10 Oct 2012
(m) U.S Coast Guard Maritime Law Enforcement Manual (MLEM), COMDTINST M16247.1 (series)
(n) Intelligence Community Directive 107, Civil Liberties, Privacy, and Transparency
(o) Administrative Investigations Manual, COMDTINST M5830.1 (series)

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 | | | | | | | | | | | | | | | | | | | | | | | | | | |
| B | x | x | | | | | | | | | | | | | | | | | | | | | | x | | |
| C | | | | | | | | | | x | | | | | | | | | | | | x | | | | |
| D | | | | | | | | | | | | | | | | | | | | | | | | | | |
| E | | | | | | | | | | | | | | | | | | | | | | x | | | | |
| F | | | | | | | | | | | | | | | | | | | | | | | | | | |
| G | | | | | | | | | | | | | | | | | | | | | | | | | | |
| H | | | | | | | | | | x | | | | | | | | | | | | | | | | |

NON-STANDARD DISTRIBUTION:

(p) Coast Guard Implementation of Presidential Policy Directive/PPD-28 – Policies and Procedures, COMDTINST M3820.5 (series)

1. PURPOSE. Intelligence oversight is a term of art that is separate and distinct from programmatic oversight. Programmatic oversight of both the Coast Guard's National Intelligence Element (NIE) and the Law Enforcement Intelligence Element (LEIE) is discussed in Reference (f) and other applicable directives. This Manual establishes policies and procedures for the oversight of Coast Guard intelligence activities and implements procedures for the conduct of intelligence oversight as described in References (a) - (p). Specifically, this Manual:

   a. Establishes policies, assigns responsibilities, and provides procedures for employee conduct and identifying, investigating, and reporting questionable intelligence activities (QIAs) and Significant or Highly Sensitive Matters (S/HSMs);

   b. Establishes policies, assigns responsibilities, and identifies procedures for inspections (ad hoc, informal, and formal), and program reviews; and

   c. Prescribes the intelligence oversight responsibilities and functions, relationships, and authorities of Coast Guard Intelligence Oversight Officials (IOOs), Coast Guard intelligence element Commanders and Directors, and the Judge Advocate General (CG-094).

2. ACTION. All Coast Guard unit commanders, commanding officers, officers-in-charge, Assistant Commandants, and Chiefs of headquarters staff elements will comply with the provisions of this Manual. Internet release is authorized.

3. DIRECTIVES AFFECTED. The Oversight of Coast Guard Intelligence Activities, COMDTINST 3821.14 is hereby cancelled. This Manual shall be read to align with References (a) – (f). In any situation where there is a conflict, follow the provisions of References (a) – (f).

4. DISCUSSION. The Coast Guard Intelligence Program consists of two parts: the NIE and the LEIE.

   a. The NIE is part of the Intelligence Community (IC) and conducts "intelligence activities" as described in References (a) and (d). Reference (c) designates the Commandant and the Assistant Commandant for Intelligence (CG-2) as the Head of the Intelligence Community (HICE) for the NIE.

   b. The LEIE conducts collection, retention, and dissemination of information pursuant to Coast Guard law enforcement and regulatory authority. Chapter 1, Paragraph A.4. of this Manual discusses the narrow circumstances in which this Manual applies to members of the LEIE.

5. DISCLAIMER. This Manual is not a substitute for applicable legal requirements, nor is it itself a rule. It is intended to provide operational guidance for Coast Guard personnel and is not intended, nor does it impose, legally binding requirements on any party outside of the Coast Guard.

   **NOTE:** Intelligence Community (IC) Inspectors General. Nothing in this Manual should be construed as impinging upon the authorities or independence of the Inspector General of the Department of Homeland Security (DHS IG), Intelligence Community Inspector General (ICIG), or any other statutory IG, as provided by Title 5, U.S.C. Appendix, as amended, also known as (and referred to

in this issuance) as "the Inspector General Act of 1978." This Manual tasks NIE Component Commanders or Directors with oversight reporting to the Judge Advocate General (CG-094) which, through assigned legal advisors, also conducts intelligence oversight inspections, and in some cases, intelligence oversight investigations. While DHS IG, ICIG, and other IGs associated with the IC may have designated intelligence oversight roles and may assist the Judge Advocate General (CG-094) with NIE or joint IC investigations, they are not required to do so.

6. MAJOR CHANGES. Major changes in this update include: Requiring supervisors of NIE Components without an assigned Legal Advisor to nominate an IOO for Judge Advocate General (CG-094) approval; providing an explanation of Intelligence Community Directive (ICD) 120; and providing implementing guidance for the requirements of ICD 120 in Enclosure (4) of this Manual.

7. IMPACT ASSESSMENT. This task will require NIE Components without an assigned Legal Advisor to nominate an IOO for the Judge Advocate General (CG-094) approval. The IOO will assist (in coordination with a legal advisor within the Office of Information and Intelligence Law (CG-LII)) the NIE Component in the administration of intelligence oversight by monitoring the accomplishment of the unit Intelligence Oversight responsibilities.

   a. The Office of Information and Intelligence Law (CG-LII) will provide training for the IOO.

   b. No additional funding will be required for this task.

8. ENVIRONMENTAL 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 DHS (CATEX) A3 from further environmental analysis, in accordance with the U.S. Coast Guard Environmental Planning Policy, COMDTINST 5090.1 and the Environmental Planning (EP) Implementing Procedures (IP).

   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 policies in this Manual must be individually evaluated for compliance with the National Environmental Policy Act (NEPA) and Environmental Effects Abroad of Major Federal Actions, Executive Order 12114, Department of Homeland Security (DHS) NEPA policy, Coast Guard Environmental Planning Policy, and compliance with all other environmental mandates.

9. 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: https://www.dcms.uscg.mil/directives/ and CGPortal: https://cgportal.uscg.mil/library/directives/SitePages/Home.aspx.

10. RECORDS MANAGEMENT CONSIDERATIONS. This Manual has been thoroughly reviewed during the directives clearance process, and determined there are no further records scheduling requirements in accordance with the Federal Records Act, 44 U.S.C. 3101 *et seq*., and 36 CFR Chapter XII, Subchapter B. This policy does not have any significant or substantial change to existing NARA records management requirements.

11. INTERNAL GUIDANCE. This issuance 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 legal prerogatives of the United States.

12. FORMS/REPORTS. None.

13. REQUEST FOR CHANGES. Units and individuals may recommend changes via the chain of command to: HQS-DG-LST-CG-LIISP@uscg.mil. All changes to this Manual will be coordinated by the Judge Advocate General (CG-094).

/MELISSA BERT/
Rear Admiral, U.S. Coast Guard
Judge Advocate General

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

This page intentionally left blank.

TABLE OF CONTENTS

## CHAPTER 1: GENERAL ISSUANCE INFORMATION

A. Applicability.

1. This Manual applies to the NIE. The NIE consists of only (i) those members in billets designated for national intelligence by the Assistant Commandant for Intelligence (CG-2) and (ii) Coast Guard components with these members assigned (NIE Components). As IC resources, the NIE must comply with the standards, direction, and guidelines of the IC as established under References (a) and (g), and are subject to References (e), (f), and this Manual.[1]

2. This Manual applies to members in billets funded by National Intelligence Program (NIP) funds. Billets funded with NIP funds are subject to intelligence oversight requirements.

3. Provisions of this Manual may also apply to any other U.S. Government or government contractor personnel acting at the direction or on behalf of a member of the NIE under authority of References (a), (e), and (f).

4. Portions of this Manual also apply to the Law Enforcement Intelligence Element (LEIE) or any other Coast Guard Personnel to the extent those personnel:

   a. Engage in activities that use intelligence sources and methods and are responsive to national intelligence requirements (e.g., open source intelligence collection (OSINT)).

   b. Engage in activities that rely in whole or in part on NIE funds or resources.

   c. Engage in activities that rely exclusively on NIE legal authority to execute.

5. Nothing in this Manual will be construed to preclude, supersede, or limit the existing authorities and policies governing the reporting of criminal or counterintelligence matters to the Coast Guard Investigative Service (CGIS), the Coast Guard Counterintelligence Service (CGCIS), or any other federal law enforcement or counterintelligence entity.

6. This Manual does not apply to the following:

   a. Any other Coast Guard organizational entity including those tasked with law enforcement, investigations, compliance, or other activity associated with the major

[1] Paragraphs 1.1.(b) and (c) of Reference (a) provide that "(b) All means, consistent with applicable United States law and this Order, and with full consideration of the rights of United States persons, shall be used to develop intelligence information for the President and the National Security Council. A balanced approach between technical collection efforts and other means should be maintained and encouraged. (c) Special emphasis should be given to detecting and countering espionage and other threats and activities directed by foreign intelligence services against the United States Government, or United States corporations, establishments, or persons." With this language, the President of the United States expanded the execution requirements under the National Intelligence Priorities Framework for the purposes of intelligence collection and oversight to include NIE Components.

operational mission programs codified in the Homeland Security Act of 2002[2] and not with national intelligence responsibilities;

b. CGIS, except as provided in Paragraph 1.A.4 above.

B. Policy.

1. Intelligence oversight requires ongoing and independent oversight of national intelligence and national intelligence-related activities.[3]

2. Appropriate senior leaders and policymakers within the Executive Branch and congressional intelligence committees must be notified of events that may erode public trust in the conduct of Coast Guard national intelligence activities.

3. In addition to applicable Executive Orders, the following officials issue intelligence oversight policy and guidance applicable to the NIE Components and the Judge Advocate General (CG-094): Director of National Intelligence (DNI), the President's Intelligence Oversight Board (IOB), and the Department of Homeland Security (DHS)/Office of the General Counsel (OGC).

4. Coast Guard intelligence oversight is conducted through five activities: (1) Training; (2) Inspections; (3) Identification, Reporting, and Investigation of Questionable Activities; (4) Periodic Reports; and (5) Executive and Congressional notifications.

5. An activity or conduct that qualifies as either a Questionable Intelligence Activity (QIA) or Significant or Highly Sensitive Matters (S/HSMs) is reportable immediately to the Judge Advocate General (CG-094). Use the reporting sequence provided in Chapter 4 of this Manual. Do not wait for substantiation, completion of an investigation, formal adjudication, or final resolution of the issue.

6. QIAs or S/HSMs reportable to the Judge Advocate General (CG-094) are not limited to those that concern U.S. persons.

7. The legal advisor assigned to NIE Components acts as the IOO for the Component. NIE Components or commands without a legal advisor that conduct national intelligence or national intelligence-related activities will nominate an IOO to be designated by the Judge Advocate General (CG-094) in accordance with Chapter 2.A.3 of this Manual.

---

[2] 6 U.S.C. 468

[3] Memorandum dated 11 Sep 2015 from the Assistant Commandant for Intelligence (CG-2), Subj: National Intelligence Program (NIP) Funding Uses, recognizes that unlike "intelligence," "intelligence-related activities" is not defined in the National Security Act of 1947 or in any other statutory or case law. It also has not been defined by the President or in Coast Guard policy. One member of the Executive Branch, the Department of Defense (DoD), defines 'intelligence related activities' as: those activities outside the consolidated defense intelligence program that: respond to operational commanders' tasking for time sensitive information on foreign entities; respond to national intelligence community tasking of systems whose primary mission is support to operating forces; train personnel for intelligence duties; provide an intelligence reserve; or are devoted to research and development of intelligence or related activities." citing (U) Dept. Of Defense, Joint Publication 2-01, Joint and National Intelligence Support to Military Operations, GL-12 (2012)). The memo also notes that intelligence training and Coast Guard intelligence reserve billets could be characterized as intelligence-related activities.

## CHAPTER 2. RESPONSIBILITIES

A. The Judge Advocate General (CG-094) and Assistant Commandant for Intelligence (CG-2) share oversight responsibilities. The Judge Advocate General (CG-094) is primarily responsible for Executive Branch reporting, while the Assistant Commandant for Intelligence (CG-2), as Head of the Intelligence Community Element (HICE), is responsible for Congressional Committee reporting.

B. Judge Advocate General of the Coast Guard (CG-094). Under the authority, policy, and direction of DNI, the IOB, and DHS/OGC, the Judge Advocate General (CG-094):

1. Conducts independent and unbiased oversight of the NIE, its national intelligence mission, and its national-intelligence-related activities. In this capacity, the Judge Advocate General (CG-094) inspects all national intelligence and national intelligence-related activities conducted by the NIE and other personnel described in Chapter 1, Paragraph A of this Manual to ensure that these activities comply with federal law, Executive Orders (EO), Presidential Directives, ICDs, and other applicable policies.

2. Develops intelligence oversight policy and, through the Office of Intelligence and Information Law (CG-LII) issues guidance to the NIE Components implementing intelligence oversight aspects of References (a) and (b).

3. Must designate in writing an IOO for each NIE Component to ensure compliance with References (a) - (l), (n), and this Manual. The IOO must have intelligence oversight as a primary duty but may be assigned other primary or collateral duties. The IOO must regularly communicate directly with the Office of Information and Intelligence Law (CG-LII) to ensure the proper conduct of oversight functions. The Judge Advocate General (CG-094) will verify the IOO has the skills, training, access and awareness to carry out that assignment prior to appointing that individual.

4. In consultation with the Assistant Commandant for Intelligence (CG-2) and the NIE Component, reviews any allegation questioning the legality or propriety of Coast Guard national intelligence and national intelligence-related activities, or where a reasonable person would believe that a national intelligence or national intelligence-related activity might be contrary to federal law, EOs, Presidential Directives, ICDs, and other applicable policies.

5. Monitors and has the first right-of-refusal to conduct administrative investigations into national intelligence and national intelligence-related activities and inspections of NIE Components; evaluates the findings; and, if appropriate, recommends corrective action to Assistant Commandant for Intelligence (CG-2) and the NIE Component concerned. In the event the Judge Advocate General (CG-094) defers to the NIE Component concerned to conduct an administrative investigation, that Component will evaluate the findings; and, if appropriate, recommend corrective action.

6. May conduct independent administrative investigations of alleged violations of law, orders, regulations, Directives, or policies as they relate to national intelligence or national intelligence-related activities. The Judge Advocate General (CG-094) will coordinate with CGIS (and/or CGCIS when there is a counterintelligence nexus) when conducting any administrative

investigation that either:

a. Initially involves an allegation of potential criminal misconduct; or

b. Once commenced, uncovers evidence of potential criminal misconduct.

7. Receives, reviews, and assesses intelligence oversight reports from the NIE Components and determines what action is required, including the fulfillment of reporting requirements.

8. The Judge Advocate General (CG-094) is the Coast Guard Senior Intelligence Oversight Official (SIOO). In this capacity, the Judge Advocate General (CG-094) is the senior official for (1) all matters associated with reports to the IOB required by References (b) and (i) (via DHS/OGC, or directly, if so designated by DHS) and (2) for addressing IOB inquiries received by Commandant (CG-2) or any NIE Component. Accordingly, the Judge Advocate General (CG-094), in coordination as necessary with other IC member intelligence oversight entities, will:

   a. Report immediately any S/HSMs involving any NIE Component. The Judge Advocate General (CG-094) will not delay reporting to DHS/OGC or the IOB any S/HSM pending completion of an investigation, command inquiry, congressional reporting, or legal proceeding.

   b. At the end of each quarter, report any QIA, S/HSM, or intelligence oversight issues reported within the quarter, including those reported previously that remain unresolved.

9. Assess and evaluate the effectiveness of NIE national intelligence and national intelligence-related activities at the request of NIE senior leadership. Conduct staff assistance visits at the request of NIE Components. Provide reports on areas of special interest to the requesting official, the NIE Component head, and DHS/OGC.

10. Have access and authority to review, any financial audit of all funds generated by NIE Component commercial activities, if any. Review and audit any funds expended by NIE Components.

11. Review NIE Component support provided to the other Coast Guard organizational entities and other U.S. Government federal departments and agencies, pursuant to Procedure 12 of Reference (e), to ensure compliance with Coast Guard intelligence oversight policy.

12. Coordinate with DHS/OGC on other matters relating to intelligence oversight.

13. Provide feedback to the NIE Components regarding intelligence oversight trends and common concerns.

14. Facilitate intelligence oversight training to NIE Components, LEIE personnel engaged in national intelligence-related activities Referenced in Chapter 1, Paragraph A.4. of this Manual, and upon request, to NIE personnel detailed to organizations outside the Coast Guard.

15. Inform the Coast Guard and/or the DHS Chief Privacy Officer, and the NIE Component concerned when, in the course of carrying out the responsibilities in this issuance, privacy or

civil liberties issues are identified.[4]

C. Assistant Commandant for Intelligence (CG-2):

1. Promptly informs the Judge Advocate General (CG-094), as the SIOO, of potential areas of concern requiring the Judge Advocate General (CG-094) attention, pursuant to the responsibilities and functions prescribed in this Manual.

2. Provides subject-matter expertise, as required, to support the Judge Advocate General (CG-094)/SIOO reporting, inspection, and investigative activities.

3. Receives and acts on substantive recommended actions associated with intelligence oversight inspection reports.

4. Mandates training requirements for the NIE and other personnel described in paragraph 1.A of this manual.

5. Makes the final determination that a reported S/HSM rises to the threshold described in Reference (i) warranting reporting to congressional intelligence committees. Within 14 days of final determination, written notification must be provided to congressional intelligence committees containing:

   a. A concise statement of the pertinent facts;

   b. An explanation of the significance of the intelligence activity; and

   c. The role of all departments and agencies involved in the intelligence activity.

D. Chief, Office of Information and Intelligence Law (CG-LII). Subject to Judge Advocate General (CG-094) supervision:

1. As the Judge Advocate General (CG-094) representative, in coordination with the Office of Intelligence Plans and Policy (CG-25) and with guidance from the Judge Advocate General (CG-094), manages oversight and compliance with Coast Guard national intelligence policy for all NIE Components and Coast Guard national intelligence activities.

2. Recommends mandated oversight training requirements for the NIE and other personnel described in Chapter 1, Paragraph A of this manual. Certifies IOOs as intelligence oversight trainers.

3. Appoints the inspectors for formal intelligence oversight inspections.

4. Verifies NIE Component nominees for the IOO position possess the skills, training, access, and awareness to carry out that assignment.

[4] Intelligence Community Directive 107, Civil Liberties, Privacy and Transparency establishes IC policy for protecting civil liberties and privacy of U.S. persons. Civil liberties and privacy are inalienable rights guaranteed by the U.S. Constitution (i.e., right to free speech, right to peacefully assemble, right to association, right to privacy, right to be free from unreasonable searches, right to travel, etc.). Reference (f) prohibits reporting intelligence information that solely describes activities protected by the U.S. Constitution.

5. Schedules and conducts formal intelligence oversight inspections. If applicable, advises Commandant (CG-2) of any substantive recommended actions.

E. Legal Advisors/IOO's. Subject to Commandant's (CG-LII) review:

1. Provide timely and accurate information to the Judge Advocate General (CG-094) on reports, investigations, and corrective actions related to QIAs and S/HSMs.

2. Prepare and review quarterly intelligence oversight reports before the NIE Component Commanding Officer or Director submits them to the Judge Advocate General (CG-094) thru Commandant (CG-LII).

3. Coordinate with the Judge Advocate General (CG-094) on the issuance of local intelligence oversight guidance to NIE Components.

4. Consult with the Judge Advocate General (CG-094) regarding any allegation questioning the legality or propriety of NIE national intelligence and Coast Guard national intelligence-related activities, or where a reasonable person would believe that the national intelligence or national intelligence-related activity may be contrary to federal law, EOs, Presidential Directives, ICDs, or other applicable policies.

5. Provide advice to the Judge Advocate General (CG-094) regarding the resolution of any disagreement by an NIE Component pertaining to investigative authority or jurisdiction for intelligence oversight investigations.

6. Review the results of all QIA and S/HSM investigations before the incident is closed and report it in the NIE quarterly intelligence oversight report.

7. Provide and document mandated intelligence oversight training.

8. In coordination with Commandant (CG-2), ensure timely reporting to Congress and the public on civil liberties, privacy, or transparency matters as may be required by federal laws, EOs, Presidential Directives, Reference (i), or as otherwise requested by the Office of the Director of National Intelligence (ODNI).

9. Provide guidance to NIE Components on proper implementation of federal law, EOs, Presidential Directives, ICDs, and other applicable policies.

10. Facilitate reporting of potential QIAs.

11. If applicable, review intelligence products prepared by NIE Components for compliance with intelligence oversight requirements prior to publication to the Intelligence Community.

12. Review requests by NIE personnel assigned to NIE Components (as opposed to intelligence organizations outside the Coast Guard) for use of special collection techniques (i.e., Procedures 5 - 10 of Reference (e)).

F. NIE Component Commanding Officers or Directors. The NIE Components conducting national intelligence or national intelligence-related activities will:

1. Develop intelligence oversight implementation guidance in coordination with the legal advisor/IOO.

2. Periodically review component-produced intelligence products for compliance with intelligence oversight requirements in coordination with the legal advisor/IOO.

3. Administer, through the legal advisor/IOO, an intelligence oversight training program that is tailored to mission requirements and provides initial and annual refresher intelligence oversight training to all NIE personnel. Determine whether intelligence oversight training should be required for non-NIE personnel of the NIE Component. At a minimum, intelligence oversight training will include:

    a. Familiarizing personnel with the authorities and restrictions established in References (a), (e), applicable ICDs, and other policies governing applicable intelligence activities; and

    b. Reporting responsibilities of NIE personnel and government contractor personnel executing NIE contracts concerning possible QIAs and S/HSMs mandated in Chapter 4 of this Manual and the protections outlined in Reference (k).

    c. A dedicated process to provide the legal advisor/IOO, on a regular basis (sufficient to meet intelligence oversight training requirements), a written summary of new and departing personnel and reporting/departing dates.

4. In accordance with the procedures in Chapter 4 of this Manual, conduct periodic comprehensive reviews of all national intelligence and national intelligence-related activities under their authority, direction, and control to verify compliance with federal law, EOs, Presidential Directives, ICDs, and other applicable policies; report significant findings to the Judge Advocate General (CG-094) thru Commandant (CG-LII).

5. Report and investigate QIAs and S/HSMs in accordance with the procedures in Chapter 4 of this Manual. Reporting will not be delayed or postponed pending an investigation, command inquiry, or legal proceeding.

6. In accordance with References (k) and (l), take no adverse action against any personnel and or contractor personnel because they intend to report, are reporting, or reported what they reasonably believe is a QIA or S/HSM.

7. Provide the NIE Component legal advisor/IOO, Commandant (CG-LII), the Judge Advocate General (CG-094), and any IG of competent jurisdiction with access to any employee(s) and to all information necessary to perform their oversight responsibilities, including information protected by special access programs, alternative compensatory control measures, or other security compartmentalization.

8. If no legal advisor is assigned to the NIE Component, nominate an IOO who: (1) is of appropriate grade and intelligence experience commensurate with his or her oversight responsibilities; (2) who has access to all Component national intelligence and national intelligence-related activities (including those protected by special access programs, alternative compensatory control measures, and other security compartments); and (3) who has direct access to the NIE Component to report on intelligence oversight compliance. The IOO assists,

in coordination with a Commandant (CG-LII) legal advisor, the NIE Component in the administration of intelligence oversight by monitoring the accomplishment of the responsibilities in this Chapter.

9. In consultation with the legal advisor/IOO, prepare an annual report to be furnished to congressional intelligence committees certifying compliance or asserting non-compliance with all application laws, EOs, directives, policies, and rules to satisfy the requirements of Section 3107 of Reference (g).

## CHAPTER 3: AUTHORITIES AND RELATIONSHIPS

Judge Advocate General of the Coast Guard (CG-094):

A. Pursuant to References (b), (e), and (h), the Judge Advocate General (CG-094) has complete and unrestricted access to all information concerning NIE Component, national intelligence and national intelligence-related activities regardless of classification or compartmentalization. This includes national intelligence special access programs, from all NIE Components and personnel, in carrying out assigned responsibilities and functions to ensure compliance with the provisions of Reference (a). If applicable, access to information in IG files must be in accordance with the Inspector General Act of 1978.[5] Access to classified information must be in accordance with the requirements of applicable security policy. TJAG's authority includes, but is not limited to:

   1. Require responsible investigative officials of an NIE Component to report QIAs; S/HSMs; allegations of improper or illegal national intelligence and national intelligence-related activities by, or within, a NIE Component; or allegations regarding a national intelligence or national intelligence-related activity that a reasonable person would believe may be contrary to a federal law, EO, Presidential Directive, ICD, or NIE issuance.

   2. Obtain information on the status, proceedings, and findings of NIE Component investigations of national intelligence and intelligence-related activities.

B. Communicates immediately and directly with DHS/OGC and/or DNI OGC as circumstances require. Communicates directly with Commandant (CG-2) as necessary, to carry out assigned responsibilities and functions, and with NIE Component personnel through NIE Component legal advisors who provide advice and counsel to their NIE Component.

C. Communicates, pursuant to DNI and DHS policy, with the IOB, the DNI OGC, and other Executive Branch and Legislative Branch officials and representatives in carrying out assigned responsibilities and functions. Ordinarily, communications with representatives of the Legislative Branch will be coordinated through Commandant (CG-2), Intelligence Strategy and Engagement Staff (CG-2X).

[5] (Pub. L. 95–452, §1, Oct. 12, 1978, 92 Stat. 1101.)

This page intentionally left blank.

## CHAPTER 4: INTELLIGENCE OVERSIGHT PROCEDURES

This Chapter provides the procedures by which the Judge Advocate General (CG-094), Commandant (CG-LII) legal advisors, and NIE Components, administer the intelligence oversight program.

A. Intelligence Oversight.

1. Intelligence Oversight Program. The purpose of intelligence oversight is to ensure that all intelligence activities are conducted in compliance with applicable U.S. law and IC policy. Likewise, the primary objective of the Coast Guard Intelligence Oversight program is to ensure that intelligence activities conducted by NIE Components and personnel comply with mandated procedures and other applicable laws and directives, and do not infringe upon or violate the rights of U.S. Persons. While oversight is primarily concerned with the rights of U.S. Persons, the oversight program and this Manual apply to all Coast Guard intelligence activities, whether they involve U.S. Persons or not.[6] The intelligence oversight program is made up of five functional areas:

   a. Identification, Reporting, and Investigation of Questionable Activities;

   b. Congressional notifications;

   c. Periodic Reports;

   d. Inspections; and

   e. Training.

B. Identification, Reporting, and Investigation of Questionable Intelligence Activities.

1. NIE personnel must immediately report any QIA or S/HSM they suspect to their chain of command or supervisor. If it is not practical to report a QIA or S/HSM to the chain of command or supervisor, reports may be made to the NIE Component legal advisor/IOO, Commandant (CG-LII), the Judge Advocate General (CG-094), DHS/OGC, or the IC Inspector General (IG).

2. NIE Component legal advisors/IOOs will act on behalf of the Judge Advocate General (CG-094) and informally survey and inspect their respective Components to determine whether such Components are involved in any QIA or S/HSM, or conduct intelligence or CI activities without an assigned mission to do so. If a survey or inspection uncovers a potential QIA or S/HSM or a potential unauthorized mission activity, the matter will be reported and investigated in accordance with Chapters 4.B through 4.E of this Manual.

3. NIE Component legal advisors/IOOs will ensure personnel are effectively trained on identifying a QIA or S/HSM and consistently comply with their intelligence oversight

[6] References (a), (e), and (f) restrict the ability of NIE Components and personnel to collect and disseminate information on U.S. Persons. For instance, Reference (e) imposes minimization requirements on Coast Guard NIE. This limitation does not apply to LEIE personnel. However, both elements are required to conduct their activities in a manner that does not violate or encroach upon the constitutional rights of U.S. Persons.

responsibilities.

4. NIE Components responsible for drafting the performance requirements (i.e., statement of work) for any contract under which contractor personnel will be conducting national intelligence or national intelligence-related activities or funding contracts under NIE authorities, will ensure that the contract requires contractor personnel to report any QIA or S/HSM to appropriate government officials identified in the contract.

C. Reporting Parameters.

1. NIE Components will report the following matters to the Judge Advocate General (CG-094) through their assigned IOO thru Commandant (CG-LII):

   a. QIAs;

   b. S/HSMs;

   c. Any Coast Guard national intelligence or national intelligence-related activity that must be reported to the U.S. Attorney General as required by law or other directive, including possible violations of federal criminal laws by employees and specific federal criminal laws by any other person as provided in procedures agreed upon by the Attorney General and the DHS/OGC;

   d. Violations of Reference (k);

   e. Violations of Reference (n); and/or

   f. Activities of Privacy and Civil Liberties Officers and/or such other civil liberties, privacy, or transparency matters as required by federal laws, EOs, Presidential Directives, Reference (i), or as otherwise requested by the Office of the Director of National Intelligence.

2. NIE Components will provide an email notification (unclassified, if possible) to the Judge Advocate General (CG-094), Commandant (CG-2), and Commandant (CG-LII), with a copy to Congressional & Governmental Affairs (CG-092), and Commandant (CG-2X) before providing briefings to any congressional committee, member of Congress, or congressional staff concerning national intelligence or national intelligence-related matters that meet the reporting criteria for QIAs, S/HSMs, or possible violations of federal criminal laws by employees and of specific federal criminal laws by any other person reported to the U.S. Attorney General. Email notification should include details concerning expected attendees and circumstances, purpose, and general nature of the briefing.

D. Investigation.

1. 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. Investigations will be convened as a Standard Investigation by the Component's Commanding Officer or Director and will be conducted in accordance with Reference (o). Investigations will require a written report that includes a description of the incident and a determination of whether the allegation was substantiated. Investigating officers will write the report in investigative report format in accordance with Reference (o). The report will include findings

of fact, opinions (to include an assessment of the cause), and recommendations (to include recommended remedial action to prevent recurrence). Written reports are to be provided to Commandant (CG-LII) upon finalization, which will provide the Judge Advocate General (CG-094) with the report upon receipt.

2. All QIAs and S/HSMs will be referred to the corresponding NIE Component or the Judge Advocate General (CG-094) for further investigation or other action under an appropriate authority. All QIAs and S/HSMs referred to a NIE Component will be reviewed by the corresponding NIE Component designated IOO to determine whether the activity is legal and consistent with applicable policy. If the IOO is not also a legal advisor, the IOO should consult the legal advisor named in the investigation convening order. Additionally, if the IOO with the guidance of the legal advisor, 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 IOO must also report the activity to the CGIS and/or the CGCIS in accordance with Coast Guard Investigative Roles and Responsibilities, COMDTINST 5520.5F; Coast Guard Counterintelligence Program, COMDTINST 3850.1; and Reference (f) as the circumstances dictate. The IOO should also refer to Coast Guard Sensitive Compartmented Information Security Administration Manual, CIM 5500.27, and follow appropriate notification procedures of actual or potential security violations, compromises, or instances of unauthorized disclosure, or exposure of SCI.

3. All QIAs and S/HSMs or other such incidents revealing the possible disclosure or potential disclosure of classified information in an unauthorized manner to a foreign power or an agent of a foreign power must be immediately reported to the Federal Bureau of Investigations (FBI), in accordance with Section 811 of the Intelligence Authorization Act. The FBI will be consulted with respect to all subsequent actions taken to determine the source of such loss or comprise and will be given complete and timely access to all employees and records necessary for purposes of investigative activities.[7] CGCIS bears the responsibility for ensuring timely reporting to the FBI.

4. Investigations will be conducted in accordance with Reference (o). Officials responsible for these investigations may obtain assistance from within the NIE Component concerned or from other NIE Components to complete such investigations in a timely manner. Any disagreement between NIE Components concerning investigative authority or jurisdiction will be raised immediately to the Judge Advocate General (CG-094) for resolution.

5. Before closing an incident in an NIE quarterly intelligence oversight report, the Judge Advocate General (CG-094) will review the results of all QIA and S/HSM investigations to assess independently the effectiveness of the investigation in identifying the cause and recommending action to prevent recurrence. Based on this review, The Judge Advocate General (CG-094) may require that the investigating authority consider additional factors or provide additional information. The Judge Advocate General (CG-094) may also initiate an independent investigation.

E. Reporting Requirements.

[7] 50 U.S.C 3381(e) (Coordination of Counterintelligence Matters with Federal Bureau of Investigation)

1. The Judge Advocate General (CG-094) is the Coast Guard senior official for all matters associated with reports to the IOB IAW reference (e). As such, the Judge Advocate General (CG-094) is responsible for the preparation of the quarterly intelligence oversight reports submitted to the President's Intelligence Oversight Board (PIOB) through DHS/OGC. These reports are prepared by Commandant (CG-LII) and describes significant CG intelligence oversight activities. The Judge Advocate General (CG-094) also responds to any requests from the PIOB concerning CG intelligence.

2. References (i) and (j) require NIE Components, thru Commandant (CG-2), to keep the congressional intelligence committees (i.e., House Permanent Select Committee on Intelligence (HPSCI) and Senate Select Committee on Intelligence (SSCI)) and the Office of the Director of National Intelligence (ODNI) "fully and currently informed" of the following intelligence activities:

   a. **Significant anticipated intelligence activities, which include:**

      (1) Intelligence activities that entail, with reasonable foreseeability, significant risk of exposure, compromise, and loss of human life;

      (2) Intelligence activities that are expected to have a major impact on important foreign policy or national security interests;

      (3) An IC element's transfer, to a recipient outside that IC element, of defense articles, personnel services, or "controlled equipment" valued in excess of $1 million as provided in Section 505 of Reference (g);

      (4) Extensive organizational changes within an IC element;

      (5) Deployment of new collection techniques that represent a significant departure from previous operations or activities or that result from evidence of significant foreign developments;

      (6) Significant activities undertaken pursuant to specific direction of the President or the National Security Council (this is not applicable to covert action, which is covered by Section 503 of Reference (g)); or

      (7) Significant acquisition, reprogramming, or non-routine budgetary actions that are of Congressional concern and that are not otherwise reportable under the NIP procedures for reprogramming and transfers.

   b. **Significant intelligence failures**: Intelligence failures that are extensive in scope, continuing in nature, or likely to have a serious impact on U.S. national security interests, and include:

      (1) The loss or compromise of classified intelligence information on such a scale or over such an extended period as to indicate a systemic loss or compromise of such information that may pose a substantial risk to U.S. national security interests;

      (2) A significant unauthorized disclosure of classified intelligence information that may

pose a substantial risk to U.S. national security interests;

(3) A potentially pervasive failure, interruption, or compromise of a collection capability or collection system; or

(4) A conclusion that an intelligence product is the result of foreign deception or denial activity, or otherwise contains major errors in analysis, with a significant impact on U.S. national security policies, programs, or activities.

c. **Significant legal interpretations**: IAW Reference (i) the Judge Advocate General (CG-094) shall notify the Congressional intelligence committees, in writing, of any significant legal interpretation of the U.S. Constitution or Federal law affecting intelligence activities conducted by the NIE, no later than 30 days after the date of commencement of any intelligence activity pursuant to such interpretation.

(1) Responsibility for determining whether a particular legal interpretation requires notification to the Congressional intelligence committees rests with the Judge Advocate General (CG-094).

(2) Each notification must include a summary of the significant legal interpretation and the intelligence activity or activities conducted pursuant to such interpretation.

(3) The Judge Advocate General (CG-094) must also provide concurrent notification to the ODNI of any notifications to Congress in this Chapter.

d. **Other significant intelligence activities which include**:

(1) Substantial changes in the capabilities or known vulnerabilities of intelligence operations or intelligence systems or resources;

(2) Programmatic developments likely to be of Congressional interest, such as major cost overruns or a major modification or termination of a significant contract;

(3) Developments that affect intelligence programs, projects, or activities that are likely to be of Congressional concern because of their substantial impact on national security or foreign policy;

(4) The loss of life in the performance of an intelligence activity;

(5) Significant developments in, or the resolution of, a matter previously reported under these procedures;

(6) An intelligence activity believed to be in violation of U.S. law, including any corrective action taken or planned in connection with such activity;

(7) Significant misconduct by an employee or contractor of an IC element that is likely to seriously affect intelligence activities or otherwise is of concern to the Congressional intelligence committees, including human rights violations;

(8) Other serious violations of U.S. criminal law by an employee of an IC element or asset, which in the discretion of the head of an IC element warrants notification to the Congressional intelligence committees;

(9) Significant activities with foreign governments and CG-2X organizations;

(10) Those likely to have significant impacts on civil liberties or privacy interests of U.S. persons.

e. The criteria described in the above paragraphs are not exhaustive. The absence of any of these criteria must not be seen as determinative. Each potential determination must be addressed on its particular merits. If it is unclear whether a notification is appropriate, NIE Components should decide in favor of notification.

f. Reference (i) also requires NIE Components to furnish congressional intelligence committees with any information, other than covert actions, within their custody or control requested by the committees to carry out their responsibilities.

g. In accordance with Section 3107 of Reference (g), NIE Components will prepare an annual report due on the 15th of December each year certifying compliance with all applicable laws, EOs, directives, policies, and rules for the calendar year to be furnished to congressional intelligence committees. If the NIE Component is unable to certify the above, it will provide a statement of the reasons it is unable to provide such a certification in sufficient detail.

F. Reporting Timelines. The NIE Components will report:

1. All S/HSMs immediately to the Judge Advocate General (CG-094) through assigned IOO. 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.

2. Quarterly Reports: 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 by the 7th day of the month following the end of the quarter to Commandant (CG-LII). Commandant (CG-LII) will then provide the reports to the Judge Advocate General (CG-094) by the 15th day of the month, unless other arrangements have been approved by the Judge Advocate General (CG-094). Quarterly reports will describe all QIAs, S/HSMs, and possible violations of federal criminal laws by employees and of specific federal criminal laws by any other person as provided in procedures agreed upon by the Attorney General and the head of the department, that were identified during the quarter. Quarterly reports are required even if no QIA or S/HSM occurred during the reporting period.

3. Biennial (Formal) Reports: The Judge Advocate General (CG-094) will conduct biennial formal inspections in a 24-month cycle that ensures each NIE Component is inspected no later than 24 months after the previous biennial inspection. There is no requirement to inspect all NIE Components in a single calendar year; rather, the cycle is flexible.

4. Unscheduled Reports: Reports may also be made immediately following informal or ad-hoc inspections or inspections performed in response to a specific incident.

G. Quarterly Reporting Format.

1. NIE Components will submit quarterly reports to Commandant (CG-LII) for the Judge Advocate General (CG-094) using the format in Enclosure (1), or a format approved by the Judge Advocate General (CG-094). The body of the report will be in signed copy. Biennial reports will be submitted to NIE Component Commanding Officers or Directors using the format in Enclosure (2) or in a format approved by the Judge Advocate General (CG-094). The body of the report will be in a signed copy.

2. The NIE Components will assign a sequential case number for each QIA and S/HSM that identifies the NIE Component and calendar year; add a suffix (either "Q" or "S" to indicate a QIA or S/HSM). For example: "CGCG-2017-04-Q" would indicate the fourth incident reported by CGCG in calendar year 2017 that is also a QIA. Use this number each time the incident is mentioned in initial reports and in updates and closeout reports.

3. The NIE Components will organize each quarterly report under the major headings of "Summary of Investigation," "Previously Reported Incidents," and "Training Statistics."

   a. The Section under "Summary of Investigation" will list all QIAs and S/HSMs reported during the quarter. If there are no new incidents the report will state that fact, will omit the subparagraphs below and resume with Paragraph 4.G.3.b (below) of this Manual (i.e., "Previously Reported Incidents"). This Section will include:

      (1) A narrative describing the incident;

      (2) A statement describing when the incident occurred, when it was initially reported within the NIE Component, and when it was reported to the Judge Advocate General (CG-094); if applicable, explain any delay in reporting;

      (3) An explanation of why the incident is considered a QIA or S/HSM, if so reported. For each QIA, identify the specific law, EO, Presidential Directive, ICD, or other applicable policy that was violated. For each S/HSM, explain why the incident could impugn the reputation of the Intelligence Community or otherwise call into question the propriety of intelligence activities;

      (4) An analysis of how or why the incident occurred, identifying the root cause;

      (5) The remedial action taken or planned to prevent recurrence of the incident. Include a description of actions taken if the incident concerns information (including U.S. Persons information) improperly acquired, handled, used, disseminated, or destroyed;

      (6) Any additional information required to provide complete and accurate reports to the Judge Advocate General (CG-094), DHS, the IOB, DNI, or to provide context about the incident; and/or

      (7) An indication of whether the incident is open or closed. If open, provide the status of the ongoing investigation. If closed, indicate whether any allegations were substantiated

or not substantiated.

b. The section under "Previously Reported Incidents" will list QIAs, S/HSMs, violations of Reference (k), and violations of Reference (n). This Section will include matters still under investigation as well as those resolved and closed during the quarter, with the same information in Paragraphs 4.H.3.a. (1) through (7) of this manual.

c. The Section under "Training Statistics" will include the following:

(1) State how many training sessions were held this quarter and how many individuals received initial training and refresher training

(2) If LEIE personnel are in a mixed NIE Component, state whether the NIE Component or IOO train LEIE personnel. (e.g., training LEIE supervisors of NIE personnel); and

(3) State the number of personnel receiving initial and refresher intelligence oversight training this quarter, and the number that are current (i.e., up to date) for both trained.

H. Intelligence Oversight Inspections:

1. The Judge Advocate General (CG-094) shall ensure authorized persons conduct regular inspections of CG NIP-funded and NIE Components to ensure compliance with applicable statutes and EOs, governing the conduct of intelligence activities, and the provisions of References (a) and (e). These inspections must not interfere with oversight inspections conducted by other authorized entities, including the IG, DHS/OGC, Community Management Staff, other IC elements, and the IOB. In addition to the timelines below, formal, and/or informal inspections may be conducted on an as needed or ad hoc basis.

2. Informal Oversight Inspection. Supervisors (i.e., Commanding Officers or Directors) of Coast Guard NIE Components must conduct informal oversight inspections on at least a semi-annual basis using the format in Enclosure (3) as a guide.

3. Formal Oversight Inspection. The Judge Advocate General (CG-094) must ensure the conduct of formal oversight inspections of all CG NIE Components on at least a biennial basis.

a. Formal oversight inspections must be conducted by personnel designated by the Judge Advocate General (CG-094), such as the IOO responsible for advising the CG NIE component concerned, or staff elements of Commandant (CG-2) with oversight expertise. In addition to the areas outlined in Enclosure (2), formal oversight inspections may cover other areas necessary to ensure compliance with References (a) and (e) and this Manual.

b. Upon completion of a formal oversight inspection, the senior inspecting official must debrief the supervisor of the CG NIE component. The senior inspecting official must summarize key findings, soliciting comments and questions, and, where appropriate, recommend changes to the component's oversight program. The senior inspecting official must complete a report of inspection for review by the supervisor. The supervisor must have ten days to provide written comments on the inspection to the senior inspecting official. Upon receipt of the supervisor's comments, if any, the senior inspecting official

must forward a final report within ten days to Commandant (CG-LII), with copies to the inspected component.

I. Criteria and Details for Inspection Reports:

Reports will have paragraphs titled:

1. Executive Summary. Using the format in Enclosure (2), provide basic information about the NIE component:

   a. Authority to conduct and purpose of inspection;

   b. Identify the inspectors and roles (e.g., lead and supporting inspectors);

   c. Current and last biennial formal intelligence oversight inspection date(s) for the NIE component;

   d. General summary, including:

      (1) Number of NIE and LEIE personnel (if applicable);

      (2) Geographic location(s) of all assigned NIE personnel;

      (3) Number of personnel interviewed and an assessment of their general awareness of intelligence oversight thresholds, and whistleblower protections; and

      (4) Descriptions of the demonstrations and tools/procedures that were provided to inspectors.

   e. Summary of any unique alignment with respect to intelligence oversight (e.g., Coast Guard Cryptologic Group and National Security Agency policy; Intelligence Coordination Center Geospatial Intelligence (GEOINT) and National Geospatial-Intelligence Agency policy)

2. Inspection Results. Required subparagraphs are:

   a. Summary: Briefly describe results of the inspection to include whether component is or is not substantially compliant with the requirements of this Manual.

   b. Training Policies and Administration: Describe how training is administered for initial and refresher training. Also, describe unit(s), which the IO is responsible for training and how training is administered to detached units, if applicable.

   c. Operations and Procedures for Collection, Retention, and Dissemination of U.S. Persons Information:

      (1) Discuss how the NIE component's operations implement procedures for the collection, retention, and dissemination (i.e., Procedures 2, 3, and 4 of Reference (e)) of U.S. Persons information. Include specific information explaining how and where it maintains records containing U.S. Persons.

(2) Discuss how the NIE component implements intelligence oversight requirements for other intelligence activities (i.e., Procedures 5 - 12 of Reference (e));

d. Oversight and Reporting of QIAs and S/HSMs: No specific content is required – look to the applicable checklists for topics and metrics under each subparagraph.

e. Privacy Compliance: Include an Enclosure to the report that reviews the applicable privacy documents required for the NIE Component, including Privacy Threshold Analyses, Privacy Impact Assessments, and System of Record Notices;

3. Best Practices. Describe best practices implemented by the NIE Component that may be considered by other NIE Components to improve intelligence oversight and/or intelligence activities.

4. Major Issue(s) and Minor Issue(s). Describe major/minor issues raised by the NIE Component or discovered by the inspectors during the inspection. Include recommendations to correct or mitigate concerns related to such issues.

5. Other Recommendations. Based on the objective findings in Paragraph 2 of Section 2, state if any suggested changes or modifications to any inspection topic in subparagraphs (a) through (d). If applicable, state whether any previous recommendations have been addressed and if not, the reason.

6. Overall Assessment. State an overall conclusion that applies the criteria drawn from the interviews/demonstrations and checklists.

7. Review Period. Provide the NIE Component Commanding Officer/Commander/Director ten (10) business days to correct or discuss any facts, findings, or recommendations. State that once the period has expired without review and/or suggested command edits, the Report will be placed in final form and signed. Provide guidance on the procedure to request an extension of the review period if needed.

8. Checklists. Inspectors will utilize the checklists in Enclosure (3) in pertinent part, depending on the component mission, to develop Paragraphs to include in the report(s).

J. ICD 120/Whistleblower Protections:

1. Whistleblowing is "the act of reporting waste, fraud, abuse and corruption in a lawful manner to those who can correct the wrongdoing."[8] IC whistleblowers are those employees or contractors working in any of the 17 elements of the IC who reasonably believe there has been a violation of law, rule, or regulation, gross mismanagement, waste of resources, abuse of authority, or a substantial danger to public health and safety. The essential distinction between whistleblowers generally and those in the IC (or those who otherwise have security clearances) is the concern for protecting classified information that may be involved in an IC-related incident or complaint. The IC has recognized that whistleblowing can save taxpayers' dollars, ensure an ethical and safe working environment, and enable timely responses for corrective action. First signed in 2014, and updated on April 29, 2016, ICD-120, Intelligence Community

[8]Congressional Research Service Report, R45345, "Intelligence Community Whistleblower Protections," updated 23 Sept 2019.

Whistleblower Protection (Enclosure (4)), provides implementing guidance for Reference (l). ICD-120 provisions include the following:

a. Protections against reprisal involving a personnel action against the IC employee making a protected disclosure.

b. Protections from reprisal for a protected disclosure that could affect an IC whistleblower's eligibility for access to classified information.

c. A requirement for each IC element to have a review process to permit appeals for any decision involving a security clearance revoked allegedly in retribution for making a lawful disclosure. The provision allows the whistleblower to maintain his or her employment status while a decision is pending.

d. Provision for an employee alleging a reprisal who has exhausted the internal agency review process to request an external review panel chaired by the IGIC.

e. A requirement for IC-wide communications and training concerning whistleblower protections.

2. Whistleblowing protections for employees and contractors in the IC are extended only to those who make a lawful disclosure. They do not cover disclosures that do not conform to statutes and directives prescribing reporting procedures intended to protect classified information, such as leaking information to the media or a foreign government. IC whistleblowing does not include a difference of opinion over policy, strategy, analysis, or priorities for intelligence funding or collection unless there is a reasonable concern over legality or constitutionality. Whistleblowing protections also do not protect against legitimate adverse personnel or security clearance eligibility decisions if the agency can demonstrate that it would have taken the same action in the absence of a protected disclosure.

3. In accordance with Reference (k), "each IC element is required to have a process for employees to seek review of personnel actions alleged to be in violation of Section A, of Reference (k). The Inspector General of the Covered Agency will conduct a review of the alleged reprisal actions as part of this process. Such review process must provide for the protection of national security information and intelligence sources and methods." The U.S. Coast Guard ICD 120 review process is contained in Enclosure (4) of this Manual.

This page intentionally left blank.

## CHAPTER 5: OVERSIGHT TRAINING FOR THE NIE AND OTHER PERSONNEL COVERED BY CHAPTER 1, PARAGRAPH A OF THIS MANUAL

A. Intelligence Oversight Training for Covered Personnel.

1. Procedure 14 of Reference (e) requires Commandant (CG-2) to ensure that CGI personnel are thoroughly familiar with Reference (a), and the provisions of References (e) and (f), and regularly trained and exercised in the application of those rules to the conduct of intelligence activities, with particular emphasis placed on Procedures 1 - 4, Procedure 14, and Procedure 15. Completion of all training must be documented in the Component's intelligence oversight records. Training records must be retained in a master file until the individual permanently departs the Component. Training activity must be reflected in quarterly Intelligence Oversight reports.

2. Initial Intelligence Oversight Training. All NIE personnel must receive initial intelligence oversight training within 30 days of their arrival at first assignment at an NIE Component, subject to deviation as determined by IOO/legal adviser. Thereafter, personnel must receive refresher training for subsequent tours. Initial training must consist of in-person training of appropriate length conducted by an instructor who has been designated in writing by the Judge Advocate General (CG-094). Training must provide instruction concerning References (a), (e)-(g), (k) and this Manual. Additional specialized training may be required by the Judge Advocate General (CG-094) and/or Commandant. "In-person" training includes any live training conducted by electronic means (e.g., telephone or videoconference).

3. NIE personnel may meet the initial intelligence oversight training requirement by completing intelligence oversight training from a variety of sources, to include the Intelligence Officer Course (IOC), Intelligence Specialist "A" School, and National Intelligence University. In addition to the requirements in this Manual, CG NIE personnel who are assigned to detached duty billets with IC partners must also satisfy the oversight training requirements of the partner component.

4. Annual Refresher Oversight Training. The training described in Paragraph 1 of this Chapter must be completed by each member of the NIE annually. This annual refresher training must occur not more than 12 months from the date of initial training or prior refresher training. The training may be led by an instructor who has been designated in writing by the Judge Advocate General (CG-094), or may be written training of appropriate length consisting of reviewing References (a), (e) - (g), (k), and this Manual with an instructor who has been designated in writing by the Judge Advocate General (CG-094) readily available (e.g., telephone or e-mail) to answer questions, or via completion of the most current "Intelligence Oversight Training Course" (presently, "COURSE DIA-CMP-2100") available in the Advanced Global Intelligence Learning Environment (AGILE). Commandant (CG-LII) may approve modification to the above requirements.

5. Corrective Intelligence Oversight Training. Corrective training must be conducted for personnel who exhibit deficiency in knowledge or understanding of References (a), (e) - (g), (k), and this Manual or to address specific oversight concerns. Such deficiencies may be identified as the result of QIAs or by other means. Corrective training must consist of in-person, verbal, or written training sufficient to correct the deficiency administered by an instructor designated in writing by the Judge Advocate General (CG-094).

## ACRONYMS

| | |
|---|---|
| AGILE | Advanced Global Intelligence Learning Environment |
| CE | Categorically Excluded |
| CGCIS | Coast Guard Counterintelligence Service |
| CGIS | Coast Guard Investigative Service |
| CG-2 | Assistant Commandant to Intelligence |
| CG-25 | Office of Intelligence Plans and Policy |
| CG-2X | Intelligence Strategy and Engagement Staff |
| CGI | Coast Guard Intelligence |
| CGIE | Coast Guard Intelligence Enterprise |
| CG-LII | Office of Information and Intelligence Law |
| DHS | Department of Homeland Security |
| DHS IG | Department of Homeland Security Inspector General |
| DHS/OGC | Department of Homeland Security Office of General Counsel |
| DNI | Director of National Intelligence |
| EO | Executive Order |
| HPSCI | House Permanent Select Committee on Intelligence |
| HSM | Highly Sensitive Matters |
| IC | Intelligence Community |
| ICD | Intelligence Community Directives |
| ICIG | Intelligence Community Inspector General |
| IG | Inspector General |
| IOB | [President's] Intelligence Oversight Board |
| IOC | Intelligence Officers Course |

| | |
|---|---|
| IOO | Intelligence Oversight Official |
| GEOINT | Geospatial Intelligence |
| LEIE | Law Enforcement Intelligence Element |
| NARA | National Archives and Records Administration |
| NEPA | National Environmental Policy Act |
| NIE | Coast Guard National Intelligence Element |
| NIP | National Intelligence Program |
| OCDNI | Office of the Director of National Intelligence |
| OGC | Office of the General Counsel |
| OSINT | Open Source Intelligence |
| PPD | Presidential Policy Directive |
| PIOB | Presidents Intelligence oversight Board |
| QIA | Questionable Intelligence Activity |
| S/HSM | Significant or Highly Sensitive Matter |
| SIOO | Senior Intelligence Oversight Official |
| SSCI | Senate Select Committee on Intelligence |

# GLOSSARY

**Executive Order (EO)**: A presidential policy Directive that implements or interprets a federal statute, a constitutional provision, or a treaty.

**Intelligence Community (IC)**: The IC is a federation of executive branch agencies and organizations that work together and separately to conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States.

**Law Enforcement Intelligence Element (LEIE):** CGI personnel that plan, direct, collect, report, process, exploit, analyze, produce, and disseminate information pursuant to Coast Guard enforcement or regulatory authorities.

**Minimization**: Coast Guard NIE access to unevaluated, raw, or un-minimized signals intelligence, including signals intelligence collected in bulk, is limited to those personnel assigned cryptologic responsibilities and subject to NSA/CSS policies. Coast Guard NIE does receive from other IC elements signals intelligence information that has been evaluated, minimized, or otherwise included in finished intelligence products subject to – among other requirements – the provisions of Presidential Policy Directive (PPD)-28.[9]

**National Intelligence:** Foreign intelligence and counterintelligence.

**National Intelligence Component**: Any organizational part of the Coast Guard National Intelligence Element.

**National Intelligence Element (NIE):** The Coast Guard NIE consists of ONLY those U.S. Coast Guard intelligence elements and persons designated by the Assistant Commandant for Intelligence (CG-2) as Intelligence Community resources as established under the National Security Act of 1947 (50 U.S.C. 401a) and are subject to *EO 12333, United States Intelligence Activities (as amended)*.

**National Intelligence Personnel:** Those Coast Guard military and civilian personnel, including contractors or other IC personnel, who are part of the Coast Guard National Intelligence Element.

**Oversight:** Regulatory supervision and/or watchful and responsible care.

**Permanent Resident Alien:** A foreign national lawfully admitted to the United States for permanent residence.

[9] Such PPD-28 provisions include those in Section 1, such as (i) the United States shall not collect signals intelligence for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion; (ii) signals intelligence shall be collected exclusively where there is a foreign intelligence or counterintelligence purpose to support national or departmental missions and not for any other purposes; (iii) it is not an authorized foreign intelligence or counterintelligence purpose to collect foreign private commercial information or trade secrets to afford a competitive advantage to U.S. companies and U.S. business sectors commercially; and (iv) signals intelligence activities shall be as tailored as feasible. If Coast Guard suspects that signals intelligence disseminated to it may have been collected or disseminated in a manner inconsistent with PPD-28, it shall so notify appropriate officials at the IC element that disseminated the SIGINT. See Reference (o).

**Questionable Intelligence Activity:** Any conduct that constitutes, or is related to, an intelligence activity that may violate the law, any executive order or presidential Directive, including *EO 12333, United States Intelligence Activities (as amended)*, or this Manual. It also includes a violation of any federal criminal law by a person assigned to CGI.

**Significant or Highly Sensitive Matter**: An intelligence or intelligence-related activity or serious criminal activity by CG NIE Component personnel that could impugn the reputation or integrity of the NIE Component or the Intelligence Community, or otherwise call into question the propriety of an intelligence activity.

**Servicing Legal Office:** The staff of the Legal Officer or office of the Judge Advocate General (CG-094) responsible for providing legal advice to the Coast Guard component concerned.

**Supervisor**: The commanding officer, director, division/branch chief, or other person directly responsible for the management and operation of a Coast Guard NIE Component.

**U.S. Person (USPER)**: A U.S. citizen; an individual known by the NIE Component concerned to be a permanent resident alien, an unincorporated association substantially composed of U.S. citizens or permanent resident aliens; and 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 USPER. A person or organization in the United States is presumed to be a USPER, 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-USPER, unless specific information to the contrary is obtained.

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

Commandant
United States Coast Guard

Unit Street Address
Mail Stop XXXX
City, State Zip Code
Staff Symbol: CG-XXXX
Phone: (xxx) xxx-xxxx
Fax: (xxx) xxx-xxxx
Email: officialemail@uscg.mil

SSIC
dd Mmm yyyy

# SAMPLE MEMORANDUM

From: Reply to
Attn of:

To:

Subj: (U) [UNIT] QUARTERLY INTELLIGENCE OVERSIGHT INSPECTION REPORT [DATE]

Ref: (a) (U) Oversight of Coast Guard Intelligence Activities, COMDTINST 3821.14A
(b) (U) Coast Guard Intelligence Activities, COMDTINST M3820.12 (series)
(c) (U) Executive Order 12333, United States Intelligence Activities, 4 Dec 1981 (as amended)
(d) (U) Intelligence Community Directive Number 112, Congressional Notification, dated 29 Jun 2017
(e) (U) Unit's Oversight Instruction
(f) (U) Other applicable Unit regulations

1. (U//FOUO) In accordance with references (a) through (f), the Coast Guard [UNIT] Intelligence Oversight Official (IOO), [NAME OF IOO], conducted an informal intelligence oversight inspection of the [UNIT] for the _____ quarter of 2020 (include dates of quarter in parenthesis i.e., 01 January through 31 March, 2020 for 1st quarter of 2020).

2. (U//FOUO) Summary of Investigation. During this quarter, [Unit] personnel reported __ potential Questionable Intelligence Activities (QIAs) or Significant or Highly Sensitive Matters (S/HSMs) in accordance with Procedure 15 of Reference (a). **OR** During this quarter, no Questionable Intelligence Activities (QIAs) or Significant or Highly Sensitive Matters (S/HSMs) were detected.

a. (U//FOUO) If an incident was discovered, describe the incident, when it occurred, when was it discovered, how was it discovered, when was it reported, when was the investigation launched, status of that investigation.

b. (U//FOUO) Include remedial or corrective actions taken or planned to prevent future occurrence of the incident.

3. (U//FOUO) Previously reported Incidents. Describe QIAs and S/HSMs still under investigation as well as those resolved and closed during the quarter.

4. (U//FOUO) Training Statistics.

a. (U//FOUO) State how many training sessions were held this quarter and how many individuals received initial training and refresher training. i.e., ___ new arrivals at [UNIT] received initial training during the ____ initial training sessions that were held this quarter. ____ individuals received the annual refresher training through [method of training: online/computer-based training, in-person refresher training sessions].

b. If LEIE personnel are in a mixed NIE Component, state whether the NIE Component or IOO train LEIE personnel. (e.g., training LEIE supervisors of NIE personnel).

c. (U//FOUO) State the total number of personnel in the unit and of that number how many are current (i.e., up-to-date) for both trainings. Provide figure as a percentage and in real numbers. i.e., _____% ([total number up to date on training] of [total number of personnel]) of [UNIT] personnel are current for initial and annual refresher training in the _____quarter of 20__.

#

Copy:

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

Commandant
United States Coast Guard

Unit Street Address
Mail Stop XXXX
City, State Zip Code
Staff Symbol: CG-XXXX
Phone: (xxx) xxx-xxxx
Fax: (xxx) xxx-xxxx
Email: officialemail@uscg.mil

SSIC
dd Mmm yyyy

# SAMPLE MEMORANDUM

From: Reply to
Attn of:

To:

Subj: [UNIT] FORMAL INTELLIGENCE OVERSIGHT INSPECTION [DATE]

Ref: (a) (U) Oversight of Coast Guard Intelligence Activities, COMDTINST 3821.14A
(b) (U) Coast Guard Intelligence Activities, COMDTINST M3820.12 (series)
(c) (U) Executive Order 12333, United States Intelligence Activities, (as amended by)
(d) (U) Executive Order 13516 of 2 Nov 2009 Amending Executive Order 13462.

1. **Executive Summary**.

   a. Authority to Conduct and purpose of Inspections.

   b. Identity of the inspectors and roles (e.g., lead and supporting inspectors);

   c. Current and last biennial formal intelligence oversight inspections date(s).

   d. General Summary to include;

      (1) Number of NIE personnel (include LEIE personnel if applicable).

      (2) Geographic locations of component.

      (3) Number of persons interviewed and an assessment of their general awareness of intelligence oversight thresholds, and whistleblower protections.

      (4) Descriptions of the demonstrations of tools/procedures that were provided to inspectors.

   e. Summary of any unique alignment with respect to intelligence oversight (e.g., CGCG and NSA policy; ICC-GEOINT and NGA policy.

2. **Inspection Results**.

a. Summary. Briefly describe results of the inspection to include whether component is or is not substantially compliant with the requirements of reference (a).

b. Training Policies and Administration. Describe how training is administered for initial and refresher training. Also describe unit(s) which the IO is responsible for training and how training is administered to detached units if applicable.

c. Operations and procedures for collection, retention, and dissemination of USPERs information.

(1) Discuss how the NIE component's operations implement procedures for the collection, retention, and dissemination (i.e., Procedures 2, 3, and 4 of reference (c)) of USPERs information; to include specific information concerning how records containing USPER information are maintained.

(2) Discuss how the NIE component implements intelligence oversight requirements for other intelligence activities (i.e., Procedures 5 - 12 of reference (c)).

d. Oversight and Reporting of QIAs and S/HSMs. No specific content is required; look to the applicable checklists for topics and metrics under each subparagraph.

e. Privacy Compliance. Include an enclosure to the report that reviews the applicable privacy documents required for the NIE component, including Privacy Threshold Analyses, Privacy Impact Assessments, and System of Record Notices.

f. Application of IO to LEIE Members. Ensure assessments account for activities of LEIE personnel to the extent they:

(1) Perform OSINT activities.

(2) Use any other national intelligence community intelligence sources or methods.

(3) Engage in activities funded in whole or in part by NIE funds (e.g., National Intelligence Program (NIP) funds).

(4) Otherwise engage in activities that rely exclusively on NIE legal authorities to execute.

3. **Best Practices**. Describe best practices implemented by the NIE component that may be considered by other NIE components to improve CG intelligence oversight and/or intelligence activities.

4. **Major Issue(s) and Minor Issue(s)**. Describe major/minor issues raised by the NIE component or discovered by the inspectors during the course of the inspection. Include recommendations to correct or mitigate concerns related to such issues.

5. **Other Recommendations**. Based on the objective findings in section 2, state any suggested changes or modifications to any inspection topic in subparagraphs (a) through (d). If

applicable, state whether any previous recommendations have been addressed and if not, the reason.

6. **Overall Assessment**. State an overall conclusion that applies the criteria drawn from the interviews/demonstrations and checklists.

#

Encl: (1) IO Checklist

Copy: CG-LII
COMDT (CG-094)

This page intentionally left blank.

# UNITED STATES COAST GUARD

# INTELLIGENCE OVERSIGHT

# ASSESSMENT/INSPECTION GUIDE & CHECKLISTS

# MARCH 2021

## ADMINISTRATIVE INFORMATION

**Unit:** _____

**Date of Assessment / Inspection:** _____

**Type of Assessment / Inspection:** ☐ **Biennial (Formal)** ☐ **Other (Spot, Ad Hoc):**_____

| Title | Name/Rank | Phone | E-Mail |
|---|---|---|---|
| Commanding Officer (CO)/Director | | | |
| Intelligence Oversight Officer (IOO) | | | |
| Alternate IOO | | | |
| Command Legal Advisor or Staff Judge Advocate (SJA) (if not the IOO) | | | |
| Senior Inspector | | | |
| Inspector | | | |
| Other (Observer, Intern) | | | |

**Unit Mission:**

_____

_____

_____

## ASSESSMENT

☐ Fail ☐ Pass w/Minimal Deficiencies ☐ Pass w/Improvement Observations ☐ Pass

/s/_____ Dated: _____
Senior Inspector

NOTE: Assessments are based on the judgment of the Senior Inspector considering the Observations and Comments, neither of which are weighted. An Inspector may issue one of four Assessments based on the Observations and their Comments in the applicable checklists below: **Fail** - significant, systemic and/or obvious deficiencies or shortcomings which have created more than one activity that met the threshold for and was reported as a Questionable Activity; **Pass w/Minimal Deficiencies** – more than one deficiency which if not corrected could be the basis for a Fail in the future, or a single activity that met the threshold for and was reported as a Questionable Activity; **Pass w/Improvement Observations** - Pass with no deficiencies but with observations and their comments that could range from minor record-keeping for training or other administrative matters, or indications that training and awareness need improvement to ambiguous or unclear policy that in the future could result in a deficiency; and **Pass – Zero deficiencies**; if Improvement Observations and Comments were noted, they were minor in nature.

**IOO PREPARATIONS**

1. When scheduled, immediately inform your chain of command of the Assessment/Inspection. Your chain of command should not be surprised to see visitors in the unit.
2. Work with the Senior Inspector and establish an agenda/calendar of events at least two weeks before the visit.
3. Be present for the Assessment/Inspection. As primary IOO, you should host the Assessment/Inspection. Do not delegate this responsibility to an alternate IOO.
4. Ensure your IO program is well-advertised (e.g., web link, Plan of the Month, smart cards, posters) and members know how to access policy and guidance.
5. Prepare unit personnel and ensure they can answer basic Intelligence Oversight Program (IOP) questions. These could include Questionable Activity reporting channels and thresholds, definitions of U.S. Persons, retention and dissemination limits, and where references and instructions are located.
6. The first event should be a brief meeting with the Commanding Officer/Director and in your discretion, department heads or supervisors such as collection managers. In some commands, the senior Command Judge Advocate (CJA)/Staff Judge Advocate (SJA) that provides general legal advice may wish to be present to observe. You should prepare these senior leaders to discuss their commitment to Intelligence Oversight. After the Command and Intelligence Oversight Brief which follows the meeting, the Senior Inspector will deliver an update on recent Intelligence Oversight issues and policy to the same senior leader audience.
7. Prepare a Command and Intelligence Oversight brief for the Inspection team and have it reviewed by your Commanding Officer or Director before the Assessment/Inspection. This should not exceed an hour and will include the agenda and explain the unit mission, authorities, and current operations. Also include a summary of Questionable Activity reporting methods and channels, planned and past intrusive collection activity (such as electronic surveillance, concealed monitoring, physical surveillance, undisclosed participation and mail cover). Brief any joint operations with other intelligence community (IC) members as well as assistance to Law Enforcement. The brief should also update the status of any Questionable Activity investigations, formal or otherwise since the last Assessment/Inspection.
8. If not already in place, prepare an IO continuity binder or electronic folder. This may be organized topically to suit your particular command and should contain previous inspection results as well as the necessary Executive Orders, Intelligence Community Directives, and statutes and policy you find essential in your IOO position. If applicable, have Questionable Activity reports and related investigations in the binder/folder. Include memoranda or documentation of corrections made to address any deficiencies/observations noted in previous Assessments/Inspections.
9. If your command is subject to other IC member policy (such as the Coast Guard Cryptologic Group (CGCG) and the National Security Agency (NSA)), be prepared to explain how your policy is consistent with that policy and its impact, if any, on your IOP.
10. Prepare unit training records and, if applicable, records of intrusive procedures and assistance to law enforcement for review.
11. Complete the Assessment/Inspection per the agenda.
12. Set up the in-person “Out Brief” by the Senior Inspector with you and your Commanding Officer/Director.
13. When the written Assessment/Inspection Report is drafted, collaborate with the Senior Inspector and be prepared to offer edits and facts for clarity. Depending on your command, be prepared to draft certain portions of the Report, such as manning and training statistics.

# INTELLIGENCE OVERSIGHT INSPECTION CHECKLIST

## COMMAND INSPECTION HISTORY AND CORRECTIONS

| Criteria | Text, Yes or No (Y/N), or Date | Observations/Comments |
|---|---|---|
| 1.*[10] Are Intelligence Oversight training and internal compliance (periodic, spot, or ad hoc) inspections included in the unit's overall policy and mission plans? | | |
| 1.a. When was the last internal periodic, spot, or ad hoc Intelligence Oversight inspection conducted by the unit IOO and/or, if applicable, participated in or was the subject of any joint or external inspection or investigation (Department of Homeland Security (DHS) Inspector General (IG), Director of National Intelligence (DNI) IG) with or by any other IC member IG? | | |
| 1.b. Are inspection reports and investigation reports identified in paragraph 1.a. in the IOO records? | | |
| 1.c. Were deficiencies and/or recommended actions noted? | | |
| 1.d. Were all deficiencies and/or recommended actions acted on? | | |
| 1.e. Were corrective actions taken? | | |
| 1.f. If in paragraph 1.a., the unit participated in or was the subject of any joint or external inspection or investigation with or by another IC member, did the IOO have adequate access to records and other information to assist? | | |
| 1.g. When was the last biennial Intelligence Oversight inspection conducted? | | |
| 1.h. Is the last Biennial Intelligence Oversight inspection report in the IOO records? | | |
| 1.i.* Were deficiencies and/or recommended actions noted? | | |
| 1.j.* Were all deficiencies and/or recommended actions acted on? | | |
| 1.k.* Were corrective actions taken? If so, what were those actions? | | |

[10] Throughout this checklist, a "*" after a line item number indicates the line item may also apply to Law Enforcement Intelligence Element (LEIE) personnel. See checklist section 13.

**INTELLIGENCE OVERSIGHT OFFICERS**

| Criteria | Text, Y/N, or Date | Comments |
|---|---|---|
| 2. If the command has a legal advisor permanently assigned, is that legal advisor the primary IOO with sole responsibility for the IOP? | | |
| 2.a. Is IOP management a primary duty or one of multiple collateral duties of the assigned legal advisor? | | |
| 2.b. Are the IOOs' duties detailed in a civilian or military billet assignment form? | | |
| 2.c. What other primary duties does the assigned legal advisor have? | | |
| 2.d. Are there any IOOs that are not the assigned legal advisor? If so, are they designated in writing by the command and do the records indicate they are certified by CG-LII? | | |
| 2.e. If because of its physical location, mission or by policy of another IC member or functional manager, the command must comply with another IC member's IOP policy for training and or/Questionable Intelligence Activity (QIA) standards, does the primary IOO have access those records? | | |
| 2.f. Does the command use alternate IOOs in either the main command structure or lower echelon commands? If so, how are they trained and what process exists to ensure transparency and access by the primary IOO? | | |
| 2.g. Are primary and alternate IOO civilian level or military ranks commensurate with their responsibilities and the overall size of the unit? | | |
| 2.h. Have primary or alternate IOOs received any in-residence Coast Guard intelligence officer training or have they completed a degree program such as that offered by the National Intelligence University? | | |
| 2.i. Where in the command organization chart is the primary IOO and who is their immediate supervisor? | | |
| 2.j. Does the primary or alternate IOO have unfettered access to: (i) procedures, programs, files, networks, databases, reporting, and data necessary for the conduct of thorough and comprehensive oversight (including information protected by special access programs, alternative compensatory control measures, and other security compartments); and (ii) access and transparency to any activity (particularly assistance to law enforcement or any joint operation with another IC member) or, operational proposal before it is tasked or executed? | | |
| 2k. Is the primary or alternate IOO in the release chain for the command's unit intelligence reporting, messages, and products prior to dissemination? If not, does the primary or alternate IOO have access to draft and finished reports, messages, and products? | | |

**INTELLIGENCE OVERSIGHT POLICY**

| Criteria | Text, Y/N, or Date | Comments |
|---|---|---|
| 3. Does the IOO have a policy to maintain an Intelligence Oversight binder for their use (online or hard copy)? | | |
| 3.a. Does the IOO have the following Intelligence Oversight essential policy documents available for IOO reference or by unit members on request? | | |
| • Executive Order 12333, as amended | | |
| • Current Coast Guard policy (COMDINST 3820.12): IC member Procedures as required by Executive Order 12333 (Intelligence Activities Manual) | | |
| • Current Coast Guard policy (COMDINST 3821.14A): Intelligence Oversight | | |
| • Current Coast Guard policy: Memorandum or SOP re: QIA reporting consistent with or attaching latest IOB CONOPS and its attached Criteria on Thresholds for Reporting Intelligence Oversight Matters | | |
| • Policy, guidelines to determine which members (military, civilians, contractors) are subject to the IOP and require training. | | |
| • Policy or an SOP to implement the IOP for remotely located or detached duty personnel | | |
| • Intelligence Community Direction 107, Civil Liberties, Privacy, and Transparency | | |
| • Intelligence Community Directive 206, Sourcing Requirements for Disseminated Analytic Products | | |
| • Intelligence Community Directive 120, Intelligence Community Whistleblower Protection | | |
| • Presidential Policy Directive 19 (PPD-19), Protecting Whistleblowers with Access to Classified Information | | |
| • Coast Guard policy (ALCOAST Commandant Notice 052/20) Open Source Interim Policy | | |
| 3.b. Is there policy to account for a mixed unit or mixed work centers, e.g., members in a Law Enforcement or Regulatory-coded billet supervising members with IC duties; and how is it determined which are subject to the IOP? Or in the alternative, is the IOO policy to train all members? | | |
| 3.c.* Is there policy to protect whistleblowers that do not violate the law who in good faith report a QIA in accordance with Coast Guard Oversight policy and/or directly to another entity that is authorized by law or Executive Branch policy to receive a QIA? | | |

**INTELLIGENCE OVERSIGHT TRAINING & STATISTICS**

| Criteria | Text, Y/N, or Date | Comments |
|---|---|---|
| 4.* Does the element have an Intelligence Oversight training program with personnel receiving both initial and refresher training? (COMDTINST 3821.14A Sec. 5.A.). | | |
| 4.a.* How is training delivered? | | |
| 4.b.* Is training tailored to the unit mission and how is it accomplished? | | |
| 4.c.* Does the IOO have a method or system to evaluate (i) the effectiveness of the training and (ii) retention / awareness of the key issues? | | |
| 4.d.* Based on questionnaires, random interviews and observations, do element personnel in general retain key issues from training sufficient to identify and report possible questionable activity? | | |
| 4.e.* How are training records maintained: spreadsheet, online, learning management, or other? | | |
| 4.f.* Are the training records current and past records archived for the minimum retention period (COMDTINST 3821.14A Sec. 5.A.1.) | | |
| 4.g. Are contractors receiving Intelligence Oversight training? | | |
| 4.h.* Are joint duty and/or detailed personnel receiving Intelligence Oversight training? | | |
| 4.g.* In some elements, personnel at all levels, including senior leadership, may have reported from either the LEIE or from a command or activity other than the Coast Guard Intelligence Program. What is the general level of Intelligence Oversight understanding and for senior leadership, do they fully support all aspects of Intelligence Oversight training? | | |
| 4.j. Do all incoming personnel receive Intelligence Oversight training within 30 days of arrival? (COMDTINST 3821.14A Sec. 5.A.1.) | | |
| 4.k.* Does the element provide the IOO with a weekly consolidated list of assigned personnel, or in the alternative is the IOO required to reconcile their records on an ad hoc basis? | | |

**TRAINING STATISTICS**

| Type | Military | Civilians | Contractors/Joint Duty/Detailees |
|---|---|---|---|
| Initial - First 30 days | Example: 47/50 or 94% | | |
| Refresher Training* | | | |
| Both Initial and Refresher | | | |

**REPORTING AND MITIGATING QUESTIONABLE INTELLIGENCE ACTIVITY (QIA)**

| Criteria | Text, Y/N, or Date | Comments |
|---|---|---|
| 5.* Does the element have a local or internal set of procedures to report QIA? (COMDTINST 3821.14A Sec. 4.B.) | | |
| 5a.* Do element personnel generally understand the reportable thresholds for reporting QIAs, e.g., violation of law, policy, or executive order? (COMDTINST 3821.14A Sec. 4.) | | |
| 5.b.* Are element personnel reporting QIA immediately upon discovery? (COMDTINST 3821.14A Sec. 4.B.) | | |
| 5.c. Are Procedure 15 (QIA) written reports (COMDTINST 3821.14A Sec. 4.C.) provided to CG-LII upon completion of investigation? | | |
| 5.d.* Are personnel aware that Procedure 15 reports may be made directly to CG-LII in the event the element IOO is absent, or if under the circumstances, it is not possible to follow the chain of command? | | |
| 5.e.* When the circumstances justify it, is the element conducting either an Administrative Investigation or Preliminary Inquiry of QIA reports? (COMDTINST 3821.14A Sec. 4.C.) | | |
| 5.f.* For both Administrative Investigations and Preliminary Inquiry of QIA reports, are they thorough, fully documented and if necessary under the circumstances, conducted by a person not assigned to the element? (COMDTINST 3821.14A Sec. 4.C.) | | |
| 5.g. What is the history of element mitigation of QIA reports such as training, and is updated local policy in place to ensure QIAs do not recur? (COMDTINST 3821.14A Sec. 4.G.(7).) | | |
| 5.h. When and if an element received Recommended Actions either at a Biennial (Formal) Inspection report, and/or thru the Judge Advocate General, does the IOO maintain a record documenting element action on the Recommended Actions? (COMDTINST 3821.14A Sec. 4.G.3.f.) | | |
| 5.i.* What matters or incidents did the element consider reporting as QIA(s), but were determined by the element to not reach the thresholds of the Intelligence Oversight Board Concept of Operations (CONOPs)? | | |

**COLLECTION/ DISSEMINATION / RETENTION OF**
**U.S. PERSON (USPER)/PERSONAL IDENTIFIABLE INFORMATION (PII)**

| Criteria | Text, Y/N or Date | Comments |
|---|---|---|
| 6.* Does the mission of the element involve the collection, retention, or dissemination of information on U.S. Persons for intelligence purposes? | | |
| 6.a. Does the element's collection of U.S. Person information meet one of the (10) ten categories in Executive Order 12333, or section 2.3 of COMDTINST 3820.12 Procedure 2? | | |
| 6.b. What is the element policy for collection, including but not limited to, any Memoranda of Agreement/Understanding, Proper Use Memoranda, or Information Sharing Agreements? | | |
| 6.c. What is the element policy for dissemination, including but not limited to, any Memoranda of Agreement/ Understanding, Proper Use Memoranda, or Information Sharing Agreements? | | |
| 6.d. What is the element policy for retention, including but not limited to, any Memoranda of Agreement/Understanding, Proper Use Memoranda, or Information Sharing Agreements? | | |
| 6.e. Do IOOs and unit personnel understand that element collection, retention and dissemination policy, including Memoranda of Agreement/Understanding, Proper Use Memoranda, or Information Sharing Agreements do are not the baseline authority to conduct intelligence activities? | | |
| 6.f.* Does element collection, retention, and dissemination policy require compliance with Executive Order 12333 and COMDTINST 3820.12 Procedure 2? | | |
| 6.g. What is the element policy to ensure the recipient of disseminated USPERS information and/or PII is entitled to receive it? | | |
| 6.h. Does the unit conduct periodic review of intelligence files and databases in order to determine if retention of USPERS information continues to be necessary to an authorized function of the element? | | |
| 6.i. What method is used to conduct the periodic file review for USPERS information? | | |
| 6.j.* What systems, files, databases or datasets does the element maintain that contain USPERS information or PII? | | |
| 6.k.* Are the systems, files, databases or datasets described in 4.j. of this document systems of records required to be compliant with the Privacy Act, and if so what is the documentation? | | |
| 6.l. Does the element possess and use any operational audio/video/tracking equipment including digital cameras, video and voice recorders, and if so what is the process to ensure data management of USPERS and/or PII is consistent with COMDTINST 3820.12 Procedures 5, 6, and 9? | | |
| 6.m. Does the periodic review described in paragraph 6.h of this document include operational audio/video/tracking equipment including digital cameras, video and voice recorders? | | |

| | | |
|---|---|---|
| 6.n. Are reviews of systems, files, databases or datasets conducted on a regular basis to ensure that USPERS information and/or PII has not been retained longer than may be authorized or necessary? (COMDTINST 3820.12 Procedure 3? | | |
| 6.o. When were the last reviews of systems, files, databases or datasets conducted and what is the documentation of the reviews? | | |

**INTRUSIVE PROCEDURES (SPECIALIZED COLLECTION TECHNIQUES)**

| Criteria | Text, Y/N, or Date | Comments |
|---|---|---|
| 7. Does the element employ special collection techniques as specified in Procedure 5 through 10? | | |
| 7.a. Is the element employing special collection techniques consistent with its mission and authorities? | | |
| 7.b. If the element has the mission and authority to employ special collection techniques, has each been approved at the level required in COMDTINST 3821.14A or at the level delegated in writing by proper authority? | | |
| 7.c. Have requests for the use of special collection techniques been reviewed and approved by the legal authority required in COMDTINST 3821.14A Sec. 2.D. | | |
| 7.d. Do operational personnel and supervisors understand and practice the "least intrusive means of collection" test before requesting approval for special collection techniques? | | |
| 7.e. If a special collection technique has been authorized for a certain period of time, has the element stayed within the approved limit? | | |
| 7.f. If any specialized collection techniques generate intelligence information reports (IIRs) or any other disseminated product, are they reviewed by the IOO prior to publication? | | |
| 7.g Has the unit requested any Procedure 10? (if so, the Inspector must review all associated documents and records) | | |
| ***Note: the inspector will review documentation (including Operational Orders (OPORDs), CONOPs, Briefs/Debriefs, Requests, After Action Reports, and Investigations, if applicable) for all special collection techniques that are both currently being active and those that have been active in the last two years.*** | | |

**ASSISTANCE TO LAW ENFORCEMENT / SPECIALIZED EQUIPMENT & EXPERT PERSONNEL**

| Criteria | Text, Y/N, or Date | Comments |
|---|---|---|
| 8 . Has the element assisted law enforcement as described in Procedure 12? | | |
| 8.a If the element assisted law enforcement via Procedure 12 was that assistance consistent with the element's mission and authorities? | | |
| 8.b If the element has assisted law enforcement via Procedure 12, has each activity been approved at the level required in COMDTINST 3820.12 or if applicable, at the level delegated in writing by proper authority? | | |
| 8.c. Have requests for assistance to law enforcement via Procedure 12 been reviewed and approved by the legal authority required in COMDTINST 3821.14A Sec. 2.A.11. | | |
| 8.d. What is the element's policy for determining whether or not: (i) equipment is "specialized;" (ii) personnel are "expert;" or (iii) information or capabilities are "technical knowledge" within the meaning of section 2.6 of Executive Order 12333? | | |
| 8.e. If the element has assisted law enforcement via Procedure 12 and it was authorized for a certain period of time, was the assistance completed within the approved period? | | |
| 8.f. If the element provided specialized equipment via Procedure 12, what were the sources and uses of appropriated funds (both National Intelligence Program (NIP) and Operating Expense (OE)) to execute the Procedure 12? | | |
| 8.g. If the element provided expert personnel via Procedure 12, what were the sources and uses of appropriated funds (both National Intelligence Program (NIP) and Operating Expense (OE)) to execute the Procedure 12? | | |
| 8.h. If the element provided technical knowledge via Procedure 12, what were the sources and uses of appropriated funds (both National Intelligence Program (NIP) and Operating Expense (OE)) to execute the Procedure 12? | | |
| 8.i. What training or briefs/debriefs/temporary additional duty endorsements are provided to element expert personnel detached for Procedure 12 duty? | | |
| 8.j. In the event element member(s) are detached for temporary duty outside the element and it is determined that the member(s) are not "expert personnel," and therefore the duty is not a Procedure 12, what training or briefs/debriefs/ temporary additional duty endorsements are provided to those members? | | |

| | | |
|---|---|---|
| 8.k. In the event element member(s) were detached for temporary duty outside the element and it is determined that the member(s) are not "expert personnel," and therefore the duty is not a Procedure 12 of COMDTINST 3821.12, what were the sources and uses of appropriated funds (both National Intelligence Program (NIP) and Operating Expense (OE)) to carry out this temporary duty? | | |
| **8.l.** ***Note: the inspector will review documentation (including OPORDs, CONOPs, Briefs/Debriefs, Requests, After Action Reports, and Investigations if applicable) for Procedure 12 assistance to law enforcement that are underway and those that have been completed in the last two years.*** | | |

**ELEMENTS WITH OPEN SOURCE INTELLIGENCE (OSINT), OPERATIONAL USE OF SOCIAL MEDIA (OSM), AND/OR MANAGED ATTRIBUTION (MA) MISSIONS**

| Criteria | Text, Y/N, or Date | Comments |
|---|---|---|
| 9.* Does the element have an authorized mission, authority, and program to conduct OSINT, OSM, and/or MA to collect foreign intelligence and/or counterintelligence? | | |
| 9.a.* List and provide documentation of each OSINT/OSM/ MA tool used by this element, including: Memoranda of Agreement, licensee and user agreement, purchase information, sponsor or provider, and relevant element policy. | | |
| 9.b.* What training is required for each OSINT/OSM/MA tool? Is training required before access is granted? | | |
| 9.c.* List and verify which element members, including contractors and joint duty/detailees, are authorized to conduct OSINT/OSM/MA. | | |
| 9.d.* Discuss the element procedures for periodic review of all OSINT/OSM/MA operations including auditing, compliance, and oversight by (if applicable) a provider or other IC member providing these capabilities. | | |
| 9.e.* Does the element maintain copies of IC, DHS, and/or Coast Guard management and policy directives for OSINT/OSM/MA? | | |
| 9.f.* Is the element compliant with applicable of IC, DHS, and/or Coast Guard policies in paragraph 9.d of this document? | | |
| 9.g.* Discuss and review any user agreements and licensing agreements for those element personnel engaged in OSNT/OSM/MA. | | |
| 9.h.* Does the IOO have access to all agreements, records, fiscal and audit data, exception reports, and technical user/licensee data for OSINT/OSM/MA from the element, providers, and (if applicable) IC members providing these capabilities? | | |

| | | |
|---|---|---|
| 9.i.* Is clear element policy in place barring members from engaging in programs other than those approved for OSINT/OSM/MA and is that policy enforced? | | |
| 9.j.* What CG-2 element is the OSINT/OSM/MA program manager and is that element managing the programs in this element? | | |
| 9.k.* If the element collects, retains, and disseminates OSINT/ OSM/MA USPERS/PII information, has the element documented that activity sufficiently for review in paragraph 6? | | |
| 9.l.* If the element collects, retains and disseminates OSINT/OSM/MA USPERS/PII information, has the element practiced proper masking/minimization requirements? | | |
| 9.m.* Has the element completed appropriate research/collection plans for OSINT collection and were these plans reviewed/approved by legal and the supervisor of the intelligence component? | | |
| 9.n.* Was the appropriate Risk Management Assessment completed for each research/collection plan described in 9.k.of this document? | | |
| ***Note: the inspector will review documentation (including OPORDSs CONOPs, Briefs/Debriefs, Requests, After Action Reports, Licensing and User Agreements and Investigations if applicable) for OSINT/OSM/MA applicable from the outset of these programs to the present day.*** | | |

**ELEMENTS WITH A COUNTERINTELLIGENCE (CI) MISSION**

| Criteria | Text, Y/N, or Date | Comments |
|---|---|---|
| 10. Does the element have an authorized mission, authority and program to conduct CI to collect foreign intelligence and/or CI? | | |
| 10.a. List and provide documentation of each technical or software tool (or equipment) used by this element for CI, including: Memoranda of Agreement, licensee and user agreement, purchase information, sponsor or provider, and relevant element policy. | | |
| 10.b. What training is required for each tool or equipment used by this element for CI? Is that training required before access is granted? | | |
| 10.c. Explain the relationship of the Coast Guard CI program with the National Counterintelligence Executive (NCIX) program, including training standards, technical capabilities, and, if applicable, certifications or qualifications granted. | | |
| 10.d. List and verify which element members, including contractors and joint duty/detailees, are authorized to conduct CI. | | |

| | | |
|---|---|---|
| 10.e. Discuss the element procedures for periodic review of all CI operations including auditing, compliance, and oversight by (if applicable) a provider or other IC member providing these capabilities. | | |
| 10.f. Does the element maintain copies of applicable IC/ NCIX, DHS, and/or Coast Guard management and policy directives for CI? | | |
| 10.g. Is the element compliant with applicable IC/ NCIX, DHS, and/or Coast Guard policies in paragraph 10.d. of this document? | | |
| 10.f. Does the element conduct CI to support CG Force Protection? If so, what is the scope and authority based on Executive Order(s), DHS, and Coast Guard policy? | | |
| 10.f. Does the element conduct CI to support Law Enforcement? If so, what is the scope of the support and under what authority are they doing so based on Executive Order(s), DHS, and Coast Guard policy? | | |
| 10.g. Does the IOO have access to all agreements, records, fiscal and audit data, exception reports, and technical user/licensee data for CI from the element, providers, and (if applicable) IC members providing these capabilities? | | |
| 10.h. Is clear element policy in place barring members from engaging in programs other than those approved for CI and is that policy enforced? | | |
| 10.i What CG-2 element is the CI program manager and is that element managing the programs in this element? | | |
| 10.j If the element collects, retains and disseminates CI USPERS/PII information, has the element documented that activity sufficiently for review in paragraph 6? | | |
| ***Note: the inspector will review documentation (including OPORDs, CONOPs, Briefs/Debriefs, Requests, After Action Reports, Licensing and User Agreements and Investigations if applicable) for CI from the outset of these programs to the present day.*** | | |

**ELEMENTS WITH A HUMAN INTELLIGENCE (HUMINT) MISSION**

| Criteria | Text, Y/N, or Date | Comments |
|---|---|---|
| 11.* Does the element have an authorized mission, authority and program to conduct HUMINT? If yes, complete section 11 below: | | |
| 11.a. * List and provide documentation of each technical or software tool (or equipment) used by this element for HUMINT, including: Memoranda of Agreement, licensee and user agreement, purchase information, sponsor or provider, and relevant element policy. | | |
| 11.b.* What training is required for each tool or equipment used by this element for HUMINT collection and is that training required before access is granted? | | |

| | | |
|---|---|---|
| 11.c.* Does the Coast Guard HUMINT program conduct activities and/or train its personnel based on Department of Defense (DoD) or Defense Intelligence Agency (DIA) policies or directives, including, but not limited to, the documents listed in section 11.c.(1)-(17), below?<br><br>If so, explain the activities, standards, and the basis for their application to the Coast Guard HUMINT program, including training standards, technical capabilities, and (if applicable) certifications or qualifications granted. | | |
| 11.c.(1).* DoD 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect U.S. Persons*, 8 Aug 2016 | | |
| 11.c.(2).* DoDD 3115.09, *DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning*, Incorporating Change 1, 15 Nov 2013 | | |
| 11.c.(3).* DoDD S-5200.37, *Management and Execution of Defense Human Intelligence (U)*, 9 Feb 2009, Incorporating Change 2, Effective 18 Nov 2013 | | |
| 11.c.(4).* DoDI S-5200.42, *Defense Human Intelligence (HUMINT) and Related Intelligence Activities* (U), 8 Dec 2009; Change 2, 16 Oct 2013 | | |
| 11.c.(5).* DoDI S-5205.01, *(U) DoD Foreign Military Intelligence Collection Activities (FORMICA)*, 9 Mar 2015 | | |
| 11.c.(6).* DoDI S-3325.07, *Guidance for the Conduct of DoD Human Source Validation (U)*, 22 Jun 2009 | | |
| 11.c.(7).* DoDD S-3325.09 - Defense Clandestine Source Operations (Ch 2), 15 Jul 2014 | | |
| 11.c.(8).* DoDI S-3325.10 - HUMINT Activities in Cyberspace - 6 Jun 2013 | | |
| 11.c.(9).* Army Regulation (AR) 381-10, *U.S. Army Intelligence Activities*, 3 May 2007 | | |
| 11.c.(10).* AR 381-100 (S), Army Human Intelligence Collection Programs (U), 15 May 1988 | | |
| 11.c.(11).* Dept. of the Army, Deputy Chief of Staff (DCS), G-2 Memorandum (S//NF), *Interim Policy Guidance for the Conduct of Oversight of Army Human Intelligence (HUMINT) Source Operations (U)*, 13 Jun 2011 | | |
| 11.c.(12).* AR 381-102 (S), U.S. Army Cover Support Program (U), 10 Jan 1991 | | |
| 11.c.(13).* AR 381-141 (C), Intelligence Contingency Funds (ICF) (U), 16 Jan 2004 | | |
| 11.c.(14).* Defense Human Intelligence Enterprise-manual (DHE-M) Vol.I 3301.001 (S//NF), Collection Requirements, Reporting, and Evaluation Procedures (U), Incorporating Change 2, 1 Feb 2012 | | |

| | | |
|---|---|---|
| 11.c.(15).* DHE-M Vol. II 3301.002 (S//NF), Collection Operations (U), 23 Nov 2010 | | |
| 11.c.(16).* Dept. of the Army (DA) Pamphlet 381-15 (S//NF), Foreign Military intelligence Collection Activities Program (U), 8 Aug 2013 | | |
| 11.c.(17).* DA Field Manual (FM) 2-22.3, (U) *Human Intelligence Collector Operations*, 6 Sep 2006 | | |
| 11.d.*Are operational proposals (OP) or concepts of operations (CONOPS) required to be submitted for review and approval before any HUMINT collection activity is conducted**?** | | |
| 11.d.* Discuss the element procedures for periodic review of all HUMINT operations including auditing, compliance, and oversight by (if applicable) a provider or other IC member (including DoD or DIA). | | |
| 11..e* Does the element maintain copies of applicable IC, DoD and DIA, DHS, and/or Coast Guard management and policy directives for HUMINT? | | |
| 11.f.* Is the element compliant with applicable IC/NCIX, DHS, and/or Coast Guard policies in paragraph 10.f. of this document? | | |
| 11.g.* Does the element conduct HUMINT to support CG Force Protection? If so, what is the scope and authority based on Executive Order(s), DHS, and Coast Guard policy? | | |
| 11.h. Does the element conduct HUMINT to support Law Enforcement? If so, what is the scope and authority based on Executive Order(s), DHS, and Coast Guard policy? | | |
| 11.h.* Does the IOO have access to all agreements, records, fiscal and audit data, exception reports, and technical user/licensee data from providers of HUMINT collection tools used by the element, and (if applicable) IC members providing these capabilities? | | |
| 11.i.* Is clear element policy in place barring members from engaging in programs other than those approved for HUMINT collection and is that policy enforced? | | |
| 11.j. What CG-2 element is the HUMINT program manager and is that element managing the programs in this element? | | |
| 11.k.* If the element collects, retains, and disseminates HUMINT containing USPERS/PII information, has the element documented that activity sufficiently for review in paragraph 6? | | |
| ***Note: the inspector will review documentation (including OPORDs, CONOPs, Briefs/Debriefs, Requests, After Action Reports, Licensing and User Agreements and Investigations if applicable) for HUMINT from the outset of these programs to the present day.*** | | |

**ELEMENTS WITH A SIGNALS INTELLIGENCE (SIGINT) MISSION**

| Criteria | Text, Y/N, or Date | Comments |
|---|---|---|
| 12. What is the source of the unit's authority to engage in a SIGINT mission? | | |
| 12.a. Does the unit provide detached duty or permanent change of station (PCS) SIGINT personnel to perform duty with a National Security Agency (NSA) element other than the Coast Guard Cryptologic Group (CGCG)? If so, describe the unit(s) and the mission. Review an unclassified organization chart that includes manning at these locations. | | |
| 12.b. Does the unit conduct a Coast Guard SIGINT mission, as approved by the Director of NSA, under delegated SIGINT Operational Tasking Authority (SOTA)? If so, provide and discuss the scope of the delegation under applicable U.S. SIGINT Directives (USSIDs). | | |
| 12.c. If the unit is currently conducting a SIGINT mission, is its authority to do so specified in valid authority documentation on file (e.g., USSID/Site Profile, Mission Delegation Form (MDF), and Staff Processing Form? Review and discuss this documentation. | | |
| 12.d. Explain the relationship of the Coast Guard Cryptologic Group with the Central Security Service (CSS) and cite whether CSS (and or another CSS member) specifies training standards, technical capabilities and, if applicable, certifications or qualifications are granted. | | |
| 12.e. Is the element commander and senior staff knowledgeable of and fulfilling their Intelligence Oversight responsibilities in accordance with (IAW) USSID 2500, 2500 SP A, and USSID 19 (Oversight and Compliance Policy)? | | |
| 12.f. Does the element have a primary and alternate IOO at all locations? If not, explain who or what entity conducts intelligence oversight at these locations. | | |
| 12.g. Are the IOOs actively involved in and do they have the requisite access, including JWICS and NSANet for awareness of the element's SIGINT mission? | | |
| 12.h. Are the primary and alternate IOOs appointed in a signed appointment from the element commander or is their position based on element policy? | | |
| 12.i. Have the IOOs completed Intelligence Oversight Officer (OVSC2201) training? (Note: This requirement is in addition to NSA/CSS Intelligence Oversight Training (OVSC1000), Oversight of Signals Intelligence Authorities (OVSC1100), and Legal Compliance and Minimization Procedures (OVSC1800) courses that are required for all members.) | | |
| 12.k. Does the senior IOO interface regularly with all element locations (including site visits to element locations performing Coast Guard SIGINT missions) and does the element provide adequate funding for this travel? | | |

| | | |
|---|---|---|
| 12.l. Does the senior IOO maintain a turnover or "smart book" with references and/or copies of required USSIDs and CSS policy and records to assist in transitions to a new IOO? | | |
| 12.m. Are there written standard operating procedures (SOPs) or instruction on file which together with the "smart book" states the role and mission of the IOO and ensures access to element records and personnel? | | |
| 12.n. Has the IOO submitted an IOO Verification Form or accepted the Intelligence Oversight lien to the NSA/CSS SID Oversight and Compliance Office (P7)? | | |
| 12.o. Has the unit submitted any SIGINT related incident reports in the past year? If yes, please complete section 12.o.(1)-(4) below: | | |
| 12.o.(1). Were the reports submitted immediately upon recognition pursuant to DoDD 5148.13 and USSID 19? | | |
| 12.o.(2). Was the commander aware of these reports and were they involved in mitigation procedures? | | |
| 12.o.(3). Was a summary of the incident(s) included in the Quarterly Intelligence Oversight Report? | | |
| 12.o.(4). Has the unit failed to report any SIGINT-related Intelligence Oversight matters? | | |
| 12.p. Has the unit submitted quarterly Intelligence Oversight reports to the Judge Advocate General (and any other required offices)? If yes, complete section 12.p.(1)-(4) below: | | |
| 12.p.(1). Were these reports submitted jointly with the P7 office? | | |
| 12.p.(2). Were these reports signed by the element commander? | | |
| 12.p.(3). Does the IOO brief the element commander in person before the reports are signed? | | |
| 12.p.(4). What is the required P7 retention period for the reports and is the element compliant with the retention requirement? | | |
| 12.q. Do SIGINT personnel have access either to current paper copies, links to on-line versions, or readily accessible files on their computers of the following documentation? If yes, complete section 12.q.(1)-(8) below:<br><br>*(Note to inspector: Only the NSA/CSS SID Policy Office may post USSIDs on-line.)* | | |
| 12.q.(1). USSID 2500 (U//FOUO) (U.S. Coast Guard – SIGINT Activities), 05 April, 2019 (U) (or most recent update) | | |
| 12.q.(2). USSID 2500, Site Profile A (U//FOUO) (Coast Guard Cryptologic Unit Texas), 03 May 2018 | | |
| 12.q.(3). USSID 18 (U)(Legal Compliance and U.S. Persons Minimization Procedures) , 25 Jan 2011 | | |

| | | |
|---|---|---|
| 12.q.(4). USSID 19 (U)(NSA/CSS Signals Intelligence Directorate – Oversight and Compliance Policy) , 13 Nov 2012 | | |
| 12.q.(5). COMDINST SM3230.2 Tactical Cryptology Manual 18 Mar 2014 | | |
| 12.q.(6). NSA/CSS Policy 1-23 (Procedures Governing NSA/CSS Activities that Affect U.S. Persons), 30 Jul 2012 | | |
| 12.q.(7). COMDINST M3812.14, *Oversight of Coast Guard Intelligence Activities*, 28 Aug 2003 | | |
| 12.q.(8). Presidential Policy Directive 28 (PDD-28), *Signals Intelligence Activities*, 17 Jan 2014 | | |
| 12.r. If able to access an NSANet or JWICs workstation, have all personnel conducting, supervising, or managing SIGINT operations received the following required on-line Intelligence Oversight training listed in 12.r.(1)-(3) below? | | |
| 12.r.(1). OVSC1000, NSA/CSS Intelligence Oversight Training | | |
| 12.r.(2). OVSC1100, Oversight of Signals Intelligence Authorities | | |
| 12.r.(3). OVSC1800, Legal Compliance and Minimization Procedures | | |
| 12.s. Do authorized personnel currently access raw SIGINT databases? If yes, complete 12.s.(1)-(4) below? | | |
| 12.s.(1). Does P7 require the element to have qualified primary and alternate auditors assigned and available to review this access? | | |
| 12.s.(2). Have auditors received OVSC3101 on-line training (this is in addition to OVSC1000, OVSC1100, and OVSC1800)? | | |
| 12.s.(3). Are auditors able to describe and demonstrate their responsibilities IAW USSID 6? | | |
| 12.s.(4). Are procedures in place to terminate a person's database access when such access is no longer required? | | |
| 12.t. Discuss unit tasking and interview the element operations officer. Review and discuss the sequence of events and steps in the approval process for element missions and complete 12.t.(1)-(3) below: | | |
| 12.t.(1). What reviews are conducted for the possibility of collections against USPERS prior to tasking? | | |
| 12.t.(2). What reviews are conducted for collections in another country's territory prior to tasking? | | |
| 12.t.(3). Does the unit issue SIGINT post-mission reports or products and if so are they reviewed by the IOO for content before release? | | |
| ***Note: the inspector may review documentation (including OPORDs, CONOPs, Briefs/Debriefs, Requests, After Action Reports, Licensing and User Agreements and Investigations if applicable) for SIGINT from the outset of these programs to the present day.*** | | |

**OVERSIGHT OF LEIE PERSONNEL ACTIVITY**

| Criteria | Text, Y/N, or Date | Comments |
|---|---|---|
| 13. Are LEIE personnel engaging in activities that trigger intelligence oversight requirements? | | |
| 13.a. Are there members of the LEIE performing OSINT activities? | | |
| 13.b. If yes, have the provisions of paragraphs 1, 3, 4, 5, 6, and 9 of this Checklist that are marked with an asterisk (*) next to the line item been applied to these LEIE members to the extent of their OSINT activities? | | |
| 13.c. Are there members of the LEIE using any other national intelligence community intelligence sources and methods? | | |
| 13.d. If "yes," have the provisions of paragraphs 1, 3, 4, 5, and 6 of this Checklist that are marked with an asterisk (*) next to the line item been applied to these LEIE members to the extent of their use of these resources? | | |
| 13.e. Are there members of the LEIE engaged in activities funded in whole or in part by NIE funds (e.g., National Intelligence Program (NIP) funds)? | | |
| 13.f. If yes, have the provisions of paragraphs 1, 3, 4, 5, and 6 of this Checklist that are marked with an asterisk (*) next to the line item been applied to these LEIE members to the extent of their participation in these functions? | | |
| 13.g. Are there members of the LEIE otherwise engaged in activities that rely exclusively on NIE legal authorities to execute? | | |
| 13.h. If "yes," have the provisions of paragraphs 1, 3, 4, 5, 6, and 11 of this Checklist that are marked with an asterisk (*) next to the line item been applied to these LEIE members the extent of their participation in these functions? | | |
| ***Note: Per COMDTINST 3820.12, only members of the NIE are authorized to engage in National Intelligence Activities. Commands must obtain a waiver from CG-2 before LEIE personnel conduct activities solely for the purpose of satisfying national intelligence requirements.*** | | |

**ENCLOSURE TO COAST GUARD INTELLIGENCE OVERSIGHT, COMDTINST M3821.14A: U.S. COAST GUARD IMPLEMENTATION OF INTELLIGENCE COMMUNITY DIRECTIVE 120 REVIEW PROCEDURES**

In accordance with Intelligence Community Directive 120, Intelligence Community Whistleblower Protection, 29 April 2016 (ICD 120), "each IC element is required to have a process for employees to seek review of personnel actions alleged to be in violation of Section A, of Presidential Policy Directive 19 (PPD19), Protecting Whistleblowers with Access to Classified Information 10 Oct 2012. The Inspector General (IG) of the Covered Agency will conduct a review of the alleged reprisal actions as part of this process. Such review process must provide for the protection of national security information and intelligence sources and methods." The U.S. Coast Guard ICD 120 review process is as follows:

A. **Filing of a complaint**. An employee in, or applicant for, a position in the Coast Guard Intelligence Enterprise (CGI) may seek review of a personnel action made against them which they allege to be in violation of ICD 120 or PPD19 by filing a complaint with Commandant (CG-LII), or the Department of Homeland Security (DHS) IG (via the DHS IG hotline or email address below).

B. **Investigation**. Within 5 working days of receiving a complaint alleging a personnel action in violation of ICD 120 or PPD19, Commandant (CG-LII) shall notify Commandant (CG-2) and TJAG and provide a copy of the written complaint to the DHS IG, ensuring that classified materials are submitted through appropriate channels. Working with Commandant (CG-2), Commandant (CG-LII) will ensure the appointment of a Preliminary Inquiry Officer (PIO) to investigate all complaints. The investigation shall be conducted in accordance with Coast Guard Administrative Investigations Manual, COMDTINST M5830.1A, dtd 7 Sep 2007, unless criminal misconduct is alleged or discovered. In cases involving allegations of criminal misconduct, Coast Guard Investigative Service (CGIS) and Coast Guard Counterintelligence Service (CGCIS) will be notified of the investigation.

C. **Determination**. Upon completion of the investigation, Commandant (CG-LII) shall provide a recommendation containing the findings to Commandant (CG-2) and Commandant (CG-094) for review. If Commandant (CG-2) and Commandant (CG-094) concur with Commandant (CG-LII)'s recommendation, Commandant (CG-094) shall forward the completed investigation to the DHS IG with a memorandum describing all actions taken and a statement concerning whether the matter is closed.

D. **Relief**. If Commandant (CG-2) and Commandant (CG-094) concur that reasonable grounds exist to believe that a personnel action occurred, exists, or has been taken, in violation of ICD 120 or PPD19, Commandant (CG-2) shall recommend that the component rescind the improper action and/or take specific corrective action to return the employee, as nearly as practicable and reasonable, to the position such employee would have held had the reprisal not occurred.

E. **Nondisclosure Agreements**. The following statement applies to non-disclosure policies, forms, or agreements of the federal government with current or former employees:

"These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive Order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive Orders and statutory provisions are controlling."

**DHS Office of the Inspector General Reporting Information**
Online: Allegation Form (Recommended)
https://www.oig.dhs.gov/hotline

Call: 1-800-323-8603 toll free
TTY: 1-844-889-4357 toll free
Fax: 202-254-4297

U.S. Mail:
DHS Office of Inspector General/MAIL STOP 0305
Attn: Office of Investigations - Hotline
245 Murray Lane SW
Washington, D.C. 20528-0305

CG-LII Contact information

Call: 202-372-2950

U.S Mail:

COMMANDANT (CG-LII)
ATTN: Office of Information and Intelligence Law
US COAST GUARD STOP 7213
2703 MARTIN LUTHER KING JR AVE SE
WASHINGTON DC 20593-7213