

NGA Instruction for The Intelligence Oversight Compliance and Awareness Program

1. References.

- a. Executive Order 12333, United States Intelligence Activities (as amended July 30, 2008).
- b. Executive Order 13462, President's Intelligence Advisory Board and Intelligence Oversight Board, February 29, 2008.
- c. NGA PD 8900R4, Policy Directive for Collection, Exploitation, and Dissemination of Information, 5 January 2004.
- d. DoD Directive 5240.01, DoD Intelligence Activities, 27 August 2007.
- e. DoD 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons, December 1982.
- f. DoD Directive 5148.11, Assistant to the Secretary of Defense for Intelligence Oversight (ATSDIO), 21 May 2004.
- g. Directive-Type Memorandum 08-052: DoD Guidance for Reporting Questionable Intelligence Activities and Significant or Highly Sensitive Matters.
- h. NGA CIO Directive 8000-022, Senior Agency Official for Privacy (SAOP).

2. Purpose. Establish the responsibilities and procedures for complying with the Intelligence Oversight (IO) responsibilities of NGA, including identifying and reporting questionable intelligence activities, specifically collection, retention, and dissemination of information concerning U.S. persons, and other prohibited activities. This instruction supersedes NI 8900.4R5, Intelligence Oversight, 30 March 2006.

3. Policy.

- a. NGA will conduct intelligence activities according to applicable IO authorities, laws, regulations, policies and procedures, employing collection techniques necessary to perform its mission. NGA will not collect, retain, or disseminate information about U.S. persons unless explicitly authorized.

(1) NGA employees will conduct intelligence activities only in accordance with applicable IO authorities, laws, regulations, policies and procedures.

(2) Where collection of information is authorized, NGA employees shall use the least intrusive collection techniques feasible for collection efforts directed within the United States or directed against U.S. persons abroad.

(3) These policies and procedures shall not apply to the collection and processing of administrative information concerning U.S. persons, such as personnel, contracting, building maintenance, construction, fiscal matters, internal accounting procedures, or disciplinary matters.

(4) No NGA employee will request any other person or entity to undertake any unauthorized intelligence activity.

(5) Violators of legal and policy guidance may be subject to administrative action. NGA may refer cases to appropriate law enforcement agencies for investigation and prosecution and/or imposition of civil or criminal penalties, as appropriate.

b. NGA employees will immediately report any questionable intelligence activity to their assigned Intelligence Oversight Officer (IOO), the NGA IO Program Management Office (IO PMO), the Office of General Counsel (OGC), the Office of Inspector General (OIG), or the Assistant to the Secretary of Defense for Intelligence Oversight (ATSDIO).

c. The NGA IO Program Management Office will ensure employees have a basic understanding of how to comply with IO responsibilities, including recognizing and reporting questionable and illegal intelligence activities. This will consist of an initial block of instruction provided to all new employees as they commence their duties and annual refresher training to maintain employees' level of knowledge about the IO program.

d. ATSDIO, the Office of the Director of National Intelligence (ODNI), and the NGA OIG will conduct periodic inspections of NGA intelligence activities. Employees will fully cooperate with both internal and external IO inspection activities.

4. Applicability and Scope. This instruction applies to all NGA employees. It describes all components of the NGA IO program— reporting, training, inspections, and investigations, and sets forth responsibilities for each NGA Directorate and Office.

5. Definitions.

a. Administrative purposes. Information is collected for "Administrative Purposes" when it is necessary for the administration of the component

concerned, but is not collected directly in performance of the intelligence activities assigned such component. Reference (e).

b. Available publicly. Information that has been published or broadcast for general public consumption, is available on request to a member of the general public, could lawfully be seen or heard by an casual observer, or is made available at a meeting open to the general public. Reference (e).

c. Collection. Information shall be considered as "collected" only when it has been received for use by an employee of a DoD intelligence component in the course of his official duties. Thus, information volunteered to a DoD intelligence component by a cooperating source would be "collected" under this procedure when an employee of such component officially accepts, in some manner, such information for use within that component. Data acquired by electronic means is "collected" only when it has been processed into intelligible form. Reference (e).

d. Consent. The agreement by a person or organization to permit DoD intelligence elements to take a particular action that affects the person or organization. Consent may be oral or written unless a specific form of consent is required for a particular procedure. Consent may be implied if adequate notice is provided that a particular action carries with it the presumption of consent to an accompanying action. Reference (e).

e. Counterintelligence. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or international terrorist activities, but not including personnel, physical, document, or communications security programs. Reference (e).

f. Dissemination. Information about U.S. persons that may be disseminated or distributed/shared, without their consent, outside of the DoD intelligence component that collected and retained the information. Does not apply to information collected solely for administrative purposes; or disseminated pursuant to law; or pursuant to a court order that otherwise imposes controls upon such dissemination. Reference (e).

g. Domestic imagery. For purposes of this Instruction, domestic imagery is national imagery covering land areas of the 50 United States, District of Columbia, U.S. territories and possessions to a 12 nautical mile seaward limit of the land area, or imagery of a wholly owned or majority held U.S. corporation on foreign soil that is the subject of collection efforts or targeting U.S. person.

h. Employee. A person employed by, assigned to, or acting for an agency including civilian and military personnel, contractors, assignees, detailees, foreign nationals, and other persons otherwise acting at the direction of such an agency.

A government employee, contract employee, individuals working for a contractor, asset, or other person or entity providing service to or acting on behalf of the Department of Defense. Reference (e).

i. Foreign intelligence. Information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counterintelligence except for information on international terrorist activities. Reference (e).

j. Intelligence activities. The collection, analysis, production, and dissemination of foreign intelligence and counterintelligence pursuant to Executive Order (EO) 12333. References (a) and (d).

k. Intelligence oversight. The process that enables NGA employees to effectively carry out their authorized functions without violating the law, any Executive Order or Presidential directive, or DoD policy and ensures that their activities affecting U.S. persons are conducted in a manner that protects the constitutional rights and privacy of those persons. Reference (e).

l. Personnel security. Measures designed to insure that persons employed, or being considered for employment, in sensitive positions of trust are suitable for such employment with respect to loyalty, character, emotional stability, and reliability and that such employment is clearly consistent with the interests of the national security. Reference (e).

m. Retention. This refers to the maintenance of information about U.S. persons that can be retrieved by reference to the person's name or other identifying data. Reference (e).

n. Questionable intelligence activities: Any conduct that constitutes, or is related to, an intelligence activity that may violate the law, an Executive order or Presidential directive, including E.O. 12333 or applicable DoD policy. Reference (d). Examples of a questionable intelligence activity include, but are not limited to the following:

- (1) Tasking intelligence personnel to conduct intelligence activities that are not part of the organization's approved mission, even if they have the technical capability to do so.
- (2) Providing intelligence services and/or products without proper authorization.
- (3) Failure to file proper use memorandum statements for imagery collection associated with U.S. persons.

(4) Collecting information on a U.S. person, even through open source, when it is not part of the organization's mission.

o. U.S. Person. A U.S. person, for purposes of this Instruction, is defined as any of the following:

(1) A United States citizen.

(2) An alien known by the DoD intelligence component concerned to be a permanent resident alien.

(3) An unincorporated association substantially composed of United States citizens or permanent resident aliens.

(4) A corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. However, a corporation or corporate subsidiary incorporated abroad, even if partially or wholly owned by a corporation incorporated in the United States, is not a United States person. References (a) and (e).

6. Responsibilities.

a. Director of NGA (D/NGA) has overall responsibility for NGA IO activities.

(1) Delegates responsibility for NGA IO activities to the NGA General Counsel.

(2) Ensures that NGA conducts intelligence activities in accordance with applicable IO authorities, laws, regulations, policies or procedures.

b. Intelligence Oversight Program Management Office (IO PMO). The IO PMO resides within the OGC and ensures that NGA conducts intelligence activities in accordance with applicable IO authorities, oversees the activities of the Intelligence Oversight Officers (IOOs), administers the IO training program, and complies with external annual/quarterly IO reporting requirements.

(1) Implements and maintains the IO program throughout NGA.

(2) Monitors trends/activities both internally and externally for impact upon NGA compliance with IO authorities, with legal guidance from OGC.

(3) Submits jointly with the OIG a Quarterly Intelligence Oversight Report to the ATSDIO describing those activities that were reasonably believed to be illegal or contrary to applicable law, authorities or regulations; actions

taken with respect to such activities; significant oversight activities during the quarter; and, any suggestions or improvements in the IO process.

(4) In coordination with OGC and OIG, updates and promulgates current policy pertaining to IO; addresses agency-wide policy issues affecting IO.

(5) Coordinates requests for exceptions or amendments to any applicable IO authorities, laws, regulations, policies and/or procedures.

(6) In coordination with OGC, develops training materials for IO training events.

(7) In coordination with OGC, assists NGA IO components as requested in developing such guidelines, working aids, training materials as are necessary to ensure compliance and promote awareness of this Instruction.

(8) In coordination with OGC, conducts IO training activities.

(9) Promotes awareness of the contents of this instruction and IO authorities/responsibilities through aggressive, proactive and sustained outreach/awareness program.

(10) Responds to IO related inquiries from external elements such as DoD, ODNI; liaises with IO counterparts from other elements from the intelligence community.

(11) Establishes and maintains a network of IOOs.

(12) Coordinates with OIG in determining whether reports of sensitive activities or significant matters are forwarded to ATSDIO and/or DoD OGC (Intelligence).

(13) Refers all reports alleging questionable intelligence activities to the NGA OIG for investigation.

(14) Assists the NGA OIG with inspections of NGA intelligence activities; reviews OIG reports of inspections and evaluates for questionable activities and noncompliance with the NGA IO program. Reviews OIG reports of investigation regarding alleged questionable activities to determine whether the activity was legal and consistent with applicable policy.

(15) Determines, as part of oversight responsibilities, if any NGA element or employee is involved in any questionable activity.

(16) Coordinates with OGC on all legal issues that arise in the course of performing these responsibilities.

c. Office of General Counsel (OGC).

- (1) Monitors the implementation of the NGA IO Program through the NGA IO Program Management Office.
- (2) Interprets applicable IO authorities, laws, regulations, policies and/or procedures; determines if any questionable activity is legal and consistent with applicable IO authorities, laws, regulations, policies and/or procedures; provides legal advice and assistance to all NGA IO components regarding activities covered by this Instruction.
- (3) Assists with the development and training of IO training materials.
- (4) Coordinates with Office of International Affairs and Policy (OIP) on domestic imagery requests and other disclosure and release related matters.
- (5) Provides input to the IO PMO regarding any IO activities undertaken during the quarter for the Quarterly Intelligence Oversight Report to ATSDIO.

d. Office of International Affairs and Policy (OIP)

- (1) Conducts annual Disclosure and Release training that enhances corporate awareness of IO.
- (2) Coordinates with OGC on proper use memoranda, domestic imagery requests, and other disclosure and release related matters.
- (3) Provides input to the IO PMO regarding any IO activities undertaken during the quarter for the Quarterly Intelligence Oversight Report to ATSDIO.

e. Office of Inspector General (OIG).

- (1) Investigates reports of questionable intelligence activities including the failure to report questionable activities or violations. Provides reports of investigation to the OGC IO Program Manager (PM) to determine if the investigated activity was legal and consistent with applicable policy. If the OGC IO PM determines that the investigated activity was not legal or consistent with applicable policy, OIG will refer the report and the OGC IO PM determination to the appropriate NGA senior management official to determine, in coordination with HD and OGC, what corrective and/or disciplinary action is required.

(2) Conducts periodic inspections of the NGA IO program implementation by NGA components. The purpose of such inspections is to determine:

(a) If the component is engaged in questionable activities.

(b) That employees within inspected components are aware of their responsibility to report questionable activities and the procedures for making such reports.

(c) If employees within inspected components have completed NGA required annual IO training.

(3) Assists with the development and implementation of established guidelines and criteria for conducting IO compliance inspections.

(4) Issues an annual inspection plan/calendar for the agency.

(5) Provides input to the IO PMO regarding any IO activities undertaken during the quarter for the Quarterly Intelligence Oversight Report to ATSDIO.

f. Acquisition Directorate (A).

(1) Ensures that contractors are informed of and comply with applicable IO authorities, laws, regulations, policies and/or procedures when their performance under contract may involve activities subject to this instruction.

(2) Includes appropriate IO warnings and protective provisions in all solicitations and contracts.

(3) Provides input to the IO PMO regarding any IO activities undertaken during the quarter for the Quarterly Intelligence Oversight Report to ATSDIO.

g. Human Development Directorate (HD)

(1) Ensure NGA's human resource information system (Peoplesoft) provides the ability to track IO training and document such in employee's personnel records.

(2) Provides input to the IO PMO regarding any IO activities undertaken and training conducted during the quarter for the Quarterly Intelligence Oversight Report to ATSDIO.

h. Office of Chief Information Officer (OCIO)

- (1) The CIO serves as NGA's Senior Agency Official for Privacy (SAOP) (Reference h) and is responsible for oversight of NGA's privacy program to ensure that privacy information maintained by the Agency is adequately protected in accordance with the Privacy Act of 1974 and the E-Government Act of 2002. As SAOP, the CIO has full responsibility and accountability for ensuring NGA's implementation of information privacy protections, including the agency's full compliance with federal laws, policies, and regulations related to information privacy (Reference h). The CIO coordinates with the IO PMO, OGC and OIG regarding privacy concerns associated with the IO compliance throughout NGA.
- (2) In coordination with the IO PMO and OGC, the CIO develops policy, guidance and training; monitors NGA-wide compliance and manages; and maintains records holding areas. The CIO ensures the authenticity and integrity of NGA records through the establishment of full life-cycle management, maintenance, and preservation techniques.
- (3) Ensures that all CIO policy guidance, training pertaining to life-cycle management, maintenance, and preservation of Agency records is in compliance with applicable IO law, authorities, and regulations.
- (4) Provides input to the IO PMO regarding any IO activities undertaken during the quarter for the Quarterly Intelligence Oversight Report to ATSDIO.

i. All Directorates and Offices.

- (1) Ensure that all intelligence activities within their assigned functions have been approved by proper authority and are conducted according to applicable IO authorities, laws, regulations, policies and/or procedures. Procurement packages submitted to AC must identify those items that may reasonably involve these intelligence activities.
- (2) Seek immediate legal review prior to any intelligence activities that, in whole or in part, raise issues of legality, consistency, or propriety.
- (3) Ensure that no employee, person, or entity is requested or tasked to undertake any unauthorized or unlawful intelligence activity.
- (4) Immediately report any questionable intelligence activity or violations. Organizations other than OIG will not conduct any inquiries or investigations into any report of questionable intelligence activity.

(5) Ensure organization personnel receive initial and annual IO training and are aware of their requirement to be familiar with applicable IO authorities, laws, regulations, policies and/or procedures, with special emphasis on the restrictions that apply to their particular operations and activities, and of their responsibility to report questionable intelligence activities and violations. No directorate or Office supervisor or manager may prohibit, or otherwise impede a subordinate's reporting of a questionable intelligence activity to the IO PM, OGC, or OIG, either directly through the designated IOO.

(6) Take appropriate administrative action regarding any employee who:

(a) Violates applicable IO authorities, laws, regulations, policies and/or procedures.

(b) Takes any reprisal action against any other employee for reporting a questionable activity or violation of authorities.

(7) Facilitate the IO PMO, OGC, OIG, and ATSDIO access to all areas, personnel, and information in order to perform their respective IO responsibilities, and ensure full cooperation of employees.

(8) Appoint IOOs for the Directorate, and subordinate Offices and units, and forward memorandums of appointment to the IO PMO.

(9) Provides input to the IO PMO regarding any IO activities undertaken during the quarter for the Quarterly Intelligence Oversight Report to ATSDIO.

j. Intelligence Oversight Officers (IOOs).

(1) Each Directorate or Office appoints a primary IOO. If necessary, additional IOOs are appointed for subordinate organizations within the Directorate or Office. The organization forwards a copy of the memorandum of appointment to the IO PMO. As a general rule, one (1) IOO should be appointed for every 20-50 employees. An IOO may be the Directorate or Office Director, or experienced and responsible individual(s) meeting each of the following criteria:

(a) Be a government civilian employee in pay band 3 or above, or a military officer in grade O-3 or above, and be able to hold the IOO position for at least one year.

(b) Have experience working with classified material.

(c) Have access eligibility for the highest level of classified information held within the Directorate or Office.

(2) Provide information regarding IO responsibilities to any employee and refer the employee to IO PMO, OGC or OIG if additional information is required. IOOs receive and forward to IO PMO, OGC, or OIG any employee report of questionable activities or violations.

(3) Serve as custodians of IO materials for their respective organization or group of employees.

(4) Facilitate and monitor completion of IO training for their respective organization or group of personnel.

(5) Provide information regarding IO responsibilities to any personnel. Refer any personnel or questions regarding IO policy and procedures to the IO PMO, OGC, or OIG, as appropriate, if additional information is required.

(6) Receive and immediately forward to the IO PMO, OGC or OIG any report of questionable intelligence activities. IOOs may refer any person directly to the IO PMO or the OIG for reporting purposes.

(7) Will not conduct any inquiry or investigation into any report of questionable intelligence activity.

(8) Be familiar with all applicable IO authorities, laws, regulations, policies and/or procedures to include the contents of this Instruction. All IOOs will be properly trained and certified by the IO PMO prior to assumption of duties.

(9) Act as the primary point of contact for their respective Directorate to the IO PMO, OGC or OIG on all IO matters to include providing input to the NGA Quarterly Intelligence Oversight Report.

k. Employees.

(1) Complete IO training annually with the intent to understand the policies and responsibilities of intelligence elements regarding the collection, retention, and dissemination of information concerning U.S. persons.

(2) Conduct intelligence activities in accordance with Executive Order 12333 (Reference a), as well as other applicable legal authorities, policies and procedures.

(3) Review the IO PMO proposals for, or questions about, intelligence activities that relate to IO authorities, laws, regulations, policies and/or procedures.

(4) Immediately report to their designated IOO, the IO PMO, the OGC or the OIG, any questionable activity or violation of applicable IO authorities, laws, regulations, policies and/or procedures.

7. Procedures.

a. General Principles. Pursuant to Reference (a) and Reference (e), Procedure 2, Collection of Information about United States Persons, information that concerns a U.S. person may be collected in order to accomplish an authorized component intelligence activity, and it falls within at least one of the following types or categories of information:

- (1) Information obtained with consent of the person concerned.
- (2) Publicly available information.
- (3) Foreign intelligence.
- (4) Counterintelligence.
- (5) Potential sources of assistance to intelligence activities.
- (6) Protection of intelligence sources and methods.
- (7) Physical security.
- (8) Personnel security.
- (9) Communications security.
- (10) Information relating to involvement in international narcotics or terrorist activities.
- (11) Threats to safety of any person or organization, including those who are targets, victims, or hostages of international terrorist organizations.
- (12) Overhead reconnaissance not directed at U.S. persons.
- (13) Administrative purposes.

b. NGA collects domestic imagery in the execution of its mission under Title 10 and Title 50, U.S. Code. Domestic Imagery collected as part of NGA's intelligence mission must be collected in accordance with the Proper Use Memorandum (PUM), Domestic Imagery Requests (DIR) process and National System for Geospatial Intelligence Manual (NSGM) CS 9400.7, Domestic Imagery.

c. Retention of Information about U.S. Persons. Information about U.S. persons may be retained if such was properly collected pursuant to one of the categories discussed above and the continued retention of this information is necessary to conduct authorized intelligence functions.

d. Temporary retention. Pursuant to Reference (e), Procedure 3, Retention of Information about United States Persons, information about U.S. persons may be retained temporarily, for a period not to exceed 90 days, solely for the purpose of determining whether that information may be permanently retained. Once a conclusive determination is made that information may not be retained, it must be destroyed. However, if the information, although not relevant to the mission of NGA, is relevant to the mission of another IC agency, it may be forwarded to that agency, consistent with other applicable IO authorities, laws, regulations, policies and/or procedures.

e. Criteria for Dissemination of information about U.S. persons. Information about U.S. persons that identifies those persons may be disseminated without the consent of those persons only under the following conditions: the information was properly collected and/or retained under the provisions of Reference (e); the recipient is reasonably believed to have a need to receive such information for the performance of a lawful governmental function, and is one of the following:

- (1) A DoD employee or contractor and has a need for such information in the course of his or her official government duties.
- (2) A law enforcement entity of Federal, State or local government, and the information may indicate involvement in activities that may violate laws that the recipient is responsible to enforce, provided that such dissemination is consistent with relevant authorities (including incidentally acquired information).
- (3) An Agency within the intelligence community.
- (4) An Agency of the Federal Government authorized to receive such information in the performance of a lawful government function.
- (5) A foreign government, and dissemination is undertaken pursuant to an agreement or other understanding with such government.

(6) Any other dissemination with proper, prior approval of General Counsel/NGA.

f. Properly Marking Records.

(1) Physical Records. Hard copy documents, articles, email that contain U.S. Person (USPER) information and has been collected and retained for intelligence purposes should be separated from personal or administrative files and properly labeled; stamp or label file/folder with "USPER"; stamp or label first page of document with "USPER" and date.

(2) Electronic Records. Soft copy documents, articles, email that contains USPER information that has been collected and retained for intelligence purposes should be separated from personal or administrative files.

g. Reporting Protocol.

(1) Questionable Intelligence Activities. In coordination with OIG, the IO PMO establishes effective procedures reporting questionable activities and ensures that all employees are aware of the IO reporting responsibility. Employees discovering a questionable intelligence activity must report such activity by contacting/notifying their IOO, the IO PMO, OGC or the OIG by the most expedient means available. Acquisition Directorate should report to their IOO, the IO PMO, or OIG any questionable activities or violations identified by contractors. IOOs report to the IO PMO, or OIG any reported questionable activity which occurred within their Directorate. The IO PMO will notify the D/NGA, the ATSDIO or DoD General Counsel (Intelligence), as appropriate. Reference (g).

(2) Significant or Highly Sensitive Matters. Intelligence activities that may or may not be unlawful or contrary to applicable IO authorities, laws, regulations, policies and procedures that could damage the reputation or integrity of the IC, or that could otherwise call into question the propriety of U.S. intelligence activities should be reported immediately to Directorate IOO, the IO PMO, OGC or OIG. The IO PMO shall notify the ATSDIO and DoD Deputy General Counsel (Intelligence) as soon as possible. ATSDIO and/or the DoD Deputy General Counsel (Intelligence) will notify the USD(I) and the Secretary, as appropriate, and notify both the Intelligence Oversight Board and ODNI Intelligence Oversight Team in a timely fashion and as appropriate. Reference (g).

(3) Significant or highly sensitive matters might be manifested in or by an activity:

(a) Involving Congressional inquiries or investigations.

- (b) That may result in adverse media coverage.
- (c) That may impact on foreign relations or foreign partners.
- (d) Related to the unauthorized disclosure of classified or protected information, such as information identifying a sensitive source and method. Reporting under this paragraph does not include reporting of routine security violations.

(4) Contents of Report of Questionable Intelligence Activity or Significant or Highly Sensitive Matters. Reports should include the following:

- (a) A narrative description of intelligence activities identified during the quarter that are reasonably believed to be unlawful or contrary to applicable IO authorities, laws, regulations, policies and/or procedures.
- (b) Why the matter is being reported:
 - (i) A potential violation of applicable IO authorities, laws, regulations, policies and/or procedures.
 - (ii) Significant or highly sensitive matter.
- (c) An explanation and analysis of how and why the incident occurred.
- (d) An assessment of any impact of the incident on national security or international relations, as well as any mitigation efforts, including success/failure of such efforts.
- (e) Any remedial action taken to prevent reoccurrence.
- (f) An assessment of any impact the reported questionable activity may have on civil liberties or protected privacy right.
- (g) How the NGA is addressing any information improperly acquired, handled, used, destroyed, as a consequence of matter being reported.
- (h) Any additional information considered relevant for purposes of fully informing the Secretary and/or Deputy Secretary of Defense, the IOB and the DNI.

(5) Periodic Reports.

(a) Quarterly Intelligence Oversight Reports. Report questionable activities not of a serious nature quarterly. Reporting periods shall be based on the calendar year. The first report for each calendar year shall cover January 1 through March 31. Succeeding reports shall follow at three month intervals. Quarterly reports are due to the ATSDIO by the 15th day of the month following the end of the quarter. Quarterly reports will describe all questionable intelligence activities as well as significant or highly sensitive matters identified during the quarter. Quarterly reports are routinely submitted to the ATSDIO through normal modes of routing and transmission. Quarterly reports are required even if no reportable matters occurred during the reporting period. Reference (g).

(b) Annual IO Report to Congress. Report questionable activities of a serious nature annually. Annual reports will describe all questionable intelligence activities, inspections, results, and trends. Substantive changes and updates will be identified in the report: training, web site maintenance, personnel changes and the IO Officers network. The OIG is required to provide input to the report. The annual report shall cover January 1 through 31 December.

(c) Contents of Report. In addition to reporting on all questionable intelligence activities as well as significant or highly sensitive matters identified during the quarter Quarterly Intelligence Oversight Reports shall include all of the following:

- (i) A summary of the gravity, frequency, trends, and patterns of matters reported for the quarter.
- (ii) Significant oversight activities undertaken and training conducted during the quarter.
- (iii) Recommendations for improvements in the intelligence oversight system.