Department of the Navy Intelligence Oversight

Commander's Handbook

UNCLASSIFIED

ALWAYS ON WATCH

INTELLIGENCE OVERSIGHT IN THE DEPARTMENT OF THE NAVY

The Department of the Navy (DON) Intelligence Oversight (IO) Program was established to ensure that intelligence and intelligence-related activities are executed in accordance with U.S. Federal Law, Executive Orders (EO), Presidential Directives, Department of Defense (DoD) directives, regulations and manuals, and Secretary of the Navy Instructions.

To ensure the security of our Nation, it is vital that we safeguard our ability to conduct intelligence and counterintelligence activities while protecting the constitutional rights of American citizens.

This DON IO Commander's Handbook is to be used as a reference tool for Navy and Marine Corps leaders and IO officials.

This Handbook summarizes relevant DoD and DON IO policies, highlights the responsibilities of key stakeholders, and outlines reporting and inspection processes.

This document does not supersede DoD or SECNAV-approved policies. If discrepancies exist between this guide and authoritative policies or regulations, the policies and regulations will take precedence.

Victor B. Minella
Deputy Under Secretary of the Navy
(Intelligence and Security)

Table of Contents

References

These documents govern Intelligence Oversight and are referenced throughout this Handbook.

Executive Order 12333, "*United States Intelligence Activities.*"

DoD Directive 5240.01, "*DoD Intelligence Activities,*" August 27, 2007, Change 3, Effective November 9, 2020.

DoD Manual 5240.01, "*Procedures Governing the Conduct of DoD Intelligence Activities,*" August 8, 2016.

DoD 5240.01-R, "*Procedures Governing the Activities of DoD Intelligence Components that affect United States Persons,*" December 1982, Change 2, Effective April 26, 2017.

DoD Directive 5148.13, "*Intelligence Oversight,*" April 26, 2017.

SECNAV Instruction 3820.3F, "*Intelligence Oversight within the Department of the Navy,*" January 2, 2020.

Key Intelligence Oversight Terms

Intelligence Activities: All activities that the DoD Components conduct pursuant to E.O. 12333

Intelligence-Related Activities:

Activities that are not conducted under the authority of EO 12333 that involve the collection, retention, or analysis of information, and the activities' primary purpose is to:

- Train intelligence personnel.
- Conduct research, development, or testing and evaluation for the purpose of developing intelligence-specific capabilities. Activities that use intelligence funding (e.g., Military Intelligence Program or National Intelligence Program) are presumed to be intelligence or intelligence-related activities.

Specifically excluded from this definition are operational security activities, such as own force monitoring, force protection, maintenance of technologies or systems, cyberspace surveillance and reconnaissance operations, and activities listed in DoDM 5240.01 Section 3.1.a.(3) along with all research, development, testing, evaluation, and training activities conducted in support of those activities. This is not an exhaustive list.

Counterintelligence (CI):

Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for, or on behalf of, foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.

Questionable Intelligence Activities (QIA):

Any intelligence or intelligence-related activity when there is reason to believe that such activity may be unlawful or contrary to an EO, Presidential Directive, Intelligence Community Directive (ICD), or applicable DoD policy governing that activity.

Significant or Highly Sensitive Matters (S/HSM):

An intelligence or intelligence-related activity (regardless of whether the intelligence or intelligence-related activity is unlawful or contrary to an EO, Presidential Directive, ICD, or DoD policy), or serious criminal activity by intelligence personnel that could impugn the reputation or integrity of the Intelligence Community (IC), or otherwise call into question the propriety of intelligence activities.

Such matters might involve actual or potential:

- Congressional inquiries or investigations.
- Adverse media coverage.
- Impact on foreign relations or foreign partners.
- Systemic compromise, loss, or unauthorized disclosure of protected information.

U.S. Persons:

- A U.S. citizen.
- An alien known by the Defense Intelligence Component concerned to be a permanent resident alien.
- An unincorporated association substantially composed of U.S. citizens or permanent resident aliens.
- A corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. A corporation or corporate subsidiary incorporated abroad, even if partially or wholly owned by a corporation incorporated in the United States, is not a U.S. person.
- A person or organization in the United States is presumed to be a U.S. person, unless specific information to the contrary is obtained. Conversely, a person or organization outside the United States, or whose location is not known to be in the United States, is presumed to be a non-U.S. person, unless specific information to the contrary is obtained.

US Person Information (USPI):

Information that is reasonably likely to identify one or more specific U.S. persons. USPI may be either a single item of information or information that, when combined with other information, is reasonably likely to identify one or more specific U.S. persons.

Determining whether information is reasonably likely to identify one or more specific U.S. persons in a particular context may require a case-by-case assessment by a trained intelligence professional. USPI is not limited to any single category of information or technology. Depending on the context, examples of USPI may include: names or unique titles; government-associated personal or corporate identification numbers; unique biometric records; financial information; and street address, telephone number, and Internet Protocol address information.

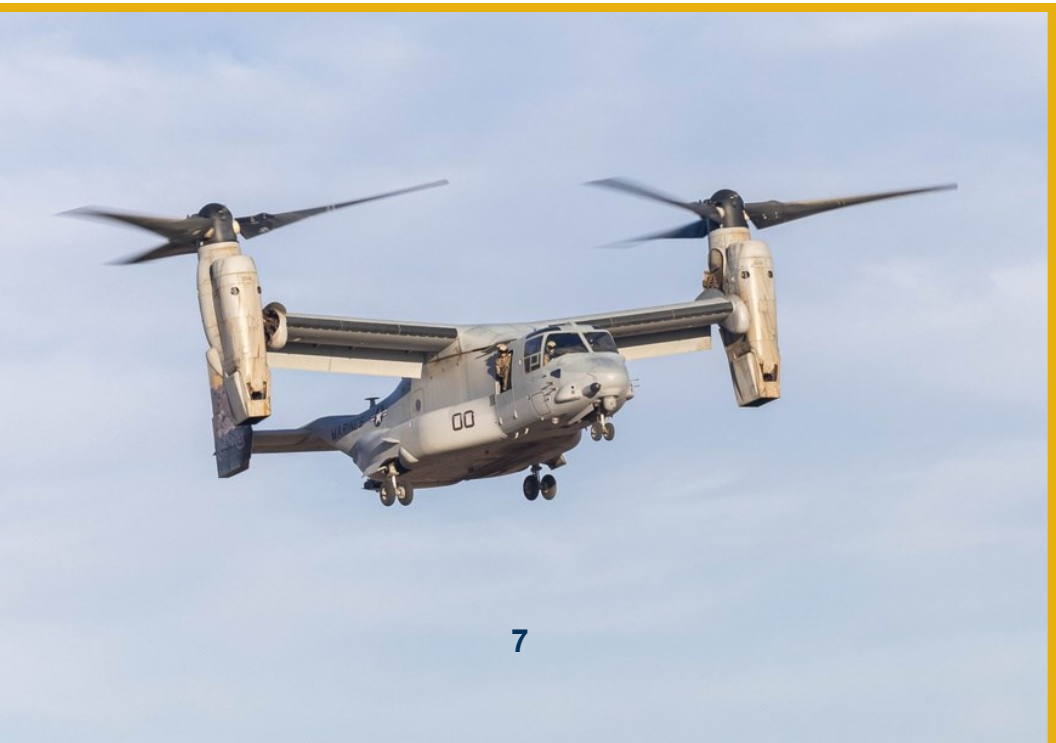
Intelligence Oversight Program

IO policies and procedures ensure the DON carries out intelligence and intelligence-related activities in compliance with U.S. law, EOs, Presidential Directives, and DoD directives, policies and regulations.

Protection of U.S. persons' privacy and civil liberties is given special emphasis to ensure DON components do not investigate U.S. persons or collect or maintain information about them solely for the purpose of monitoring activities protected by the First Amendment.

As the DON Senior Intelligence Oversight Official (SIOO), the Senior Director of Intelligence, Deputy Under Secretary of the Navy (Intelligence and Security) (DUSN (I&S)) assists the Secretary of the Navy in performing the statutory responsibility to provide oversight, governance, and management of DON intelligence activities.

The Deputy Chief of Naval Operations for Information Warfare (OPNAV N2/N6) and Marine Corps Deputy Commandant for Information (DC-I), authorize collection, retention, and dissemination of U.S. persons information (USPI), through



their designations in EO 12333 as Heads of Intelligence Community Elements (HICE).

Commanders, directors, and heads of activities are responsible to ensure compliance as described in SECNAVINST 3820.3F and to report all QIAs and Significant/ Highly Sensitive Matters (S/HSMs) to the DON SIOO via their chain of command.

Roles and Responsibilities

Commanders, commanding officers, directors, and heads of activities are responsible for complying with SECNAV Guidance and Instructions pertaining to IO to include:

- Appoint an Intelligence Oversight Officer (IOO) of a grade and experience commensurate with their oversight responsibilities.
- Establish processes and procedures for the periodic and comprehensive review of all intelligence and intelligence-related activities under the organization's authority, direction, and control.
- Ensure legal reviews are conducted.
- Administer a tailored IO training program.
- Submit S/HSM immediately, and QIA via their Quarterly IO reports.
- Ensure the cognizant Inspector General (IG) inspects organization at an interval of no greater than once every 36 months, with appropriate follow-up or assistance between inspections, as necessary.
- Report to NCIS all possible violation of federal criminal law.
- Provide access to all intelligence and intelligence-related activities to appropriately cleared IG and legal representatives conducting IO responsibilities.
- Ensure all subordinate intelligence components, units, and elements in or under their command comply with the requirements of SECNAVINST 3820.3F.

Intelligence Oversight Procedures

Procedure 1. General Provisions:

Defense Intelligence Components provide necessary information about activities, capabilities, plans, and intentions of foreign powers, organizations, persons, and their agents.

The procedures in this issuance govern the conduct of Defense Intelligence Components (hereafter, a "Component") and non-intelligence components or elements, or anyone acting on behalf of those components or elements, when conducting intelligence activities under DoD authorities.

Procedure 2. Collection of USPI:

Specifies the general criteria governing the collection of USPI.

Intentional Collection of USPI only if the information sought is reasonably believed to be necessary for the performance of an authorized intelligence mission or function assigned to the Component, and the USPI must fall within 1 of the 13 following categories:

- Publicly Available
- Consent
- Foreign Intelligence (Includes international narcotics)
- Counterintelligence
- Threats to safety (foreign connections, imminent danger, etc)
- Protection of intelligence sources, methods, or activities – DoD affiliated
- Current, former, or potential sources of assistances to intelligence activities
- Persons in contact with potential sources
- Personnel Security
- Physical Security

- Communications Security investigation
- Overhead/Airborne reconnaissance not directed at specific U.S. persons
- Administrative Purposes

Procedure 3. Retention of USPI:

Governs the retention of USPI collected by Defense Intelligence Components in accordance with Procedure 2. USPI information will be evaluated by the DoD Intelligence Component (DIC) to determine if it should be permanently retained.

Intentional Collection: Up to 5 years (must be promptly evaluated)

Incidental Collection:

- In the U.S.: Up to 5 years
- Outside the U.S.: Up to 25 years

Voluntarily Provided:

- Reasonably believed to USP: Up to 5 years (must be promptly evaluated)
- Reasonably believed to Non-USPI collection that may contain USPI: Up to 25 years

Special Circumstances:

- Up to 5 years (Must be promptly evaluated if intentional)

Extended Retention: No more than 5 additional years

- Approved by Intelligence Component Head
- No extension for 25 year retention files

Procedure 4. Dissemination of USPI:

Governs the dissemination of USPI collected or retained by a Component. Information may be disseminated pursuant to this procedure only if it was properly collected or retained in accordance with Procedures 2 or 3. This procedure applies to

USPI in any form, including physical and electronic files and information a Component places in databases, on websites, or in shared repositories accessible to other persons or organizations outside the Component.

Procedure 5. Electronic Surveillance:

Implements FISA and E.O. 12333. A Component may conduct electronic surveillance for an intelligence purpose in accordance with FISA or EO 12333 and this procedure.

The legal framework for conducting electronic surveillance is dependent upon the Component's mission, the U.S. person status and location of the target, the methods used to conduct the electronic surveillance, and the type of communication sought. All electronic surveillance must also comply with Procedures 1 through 4 of this issuance.

Procedure 6. Concealed Monitoring:

Governs concealed monitoring of any person inside the United States or any U.S. person outside the United States for an authorized FI or CI purpose by a Component or anyone acting on their behalf.

This procedure does not apply to concealed monitoring conducted as part of testing or training exercises when the subjects are participants who have consented to the concealed monitoring as part of an approved testing or training plan. A Component may, however, collect, retain, and disseminate USPI in the course of such concealed monitoring only if otherwise authorized by this issuance.

Procedure 7. Physical Searches:

Applies to nonconsensual physical searches for intelligence purposes of any person or property in the United States and of U.S. persons or their property outside the United States that are conducted by Components or anyone acting on their behalf.

Procedure 8. Searches of Mail and the use of Mail Covers:

Governs the physical searches of mail, including the opening or other examination of the content of mail, in the United States and abroad, by a Component or anyone acting on its behalf.

This procedure also applies to the use of mail covers. Mail covers are the non-consensual recording of any data appearing on the outside cover of any sealed or unsealed mail matter.

A Component may only search mail or use a mail cover if such activity is for an authorized FI or CI purpose. This procedure does not apply to items transported by a commercial carrier (e.g., Federal Express or the United Parcel Service). Such items are subject to the provisions of Procedure 7.

Procedure 9. Physical Surveillance:

Governs physical surveillance of any person inside the United States or any U.S. person outside the United States by a Component or anyone acting on their behalf.

If anyone acting on behalf of a Component conducts physical surveillance, this procedure applies to any devices such person operates to observe subject of surveillance, and not the provisions of Procedure 6.

This procedure does not apply to physical surveillance conducted as part of testing or training exercises when the subjects are participants in an exercise who have consented to the surveillance as part of an approved testing or training plan. It also does not apply to surveillance detection or counter surveillance activities in which Component personnel must detect and elude foreign physical surveillance.

A Component may, however, collect, retain, and disseminate USPI in the course of surveillance detection or counter surveillance activities only if otherwise authorized by this issuance.

Procedure 10. Undisclosed Participation (UDP) in Organizations:

Governs the participation by Components and anyone, including sources, acting on behalf of a Component in any organization in the United States or organization outside the United States that constitutes a U.S. person.

Anyone acting on behalf of a Defense Intelligence Components (including sources) may join, become a member of, or participate in an U.S. Person defined organization, **IF** their intelligence affiliation is disclosed to an appropriate official in that organization.

There are four levels of approval, depending on the nature of intended participation:

- No specific approval required
- Approved by Defense Intelligence Components Head or Delegee
- Approved by Defense Intelligence Components Head or Single Delegee
- Approved by USD(I&S)

Procedure 10 covers undisclosed participation in these organizations and is complicated! Seek advice of your JAG

Procedure 11. Contracting for Goods and Services:

Applies to contracting or other arrangements with United States persons for the procurement of goods and services by Components within the United States.

This procedure does not apply to contracting with government entities, or to the enrollment of individual students in academic institutions. The latter situation is governed by Procedure 10.

Procedure 12. Provision of Assistance to Law Enforcement Authorities:

Applies to the provision of assistance by Components to law enforcement authorities. It incorporates the specific limitations on such assistance contained in E.O. 12333 together with the general limitations and approval requirements of DoD Directive 5525.5.

Procedure 13. Experimentation on Human Subjects for Intelligence Purposes:

Applies to experimentation on human subjects if such experimentation is conducted by or on behalf of a Component.

This procedure does not apply to experimentation on animal subjects.

Reporting Requirements

In accordance with SECNAVINST 3820.3F, DON component commands (Echelon 1-2) must submit Quarterly IO Reports to the DON SIOO (DUSN (I&S), Senior Director for Intelligence). The Quarterly Intelligence Oversight Report Format Template can be found in SECNAVINST 3820.3F, enclosure 3.

S/HSM will be submitted immediately and both QIAs and S/HSMs will be submitted quarterly to the DON SIOO.

Reportable activities are not limited to those that concern U.S. persons.

Reports requiring SAP protection will be coordinated through DON SAPCO/OPNAV N9SP.

Note: When a QIA or S/HSM results in significant intelligence failure, DoD SIOO notifies the President's Intelligence Oversight Board, and the Component or USD (I&S) may notify Congress.

Quarterly Intelligence Oversight Report Format includes:

- ☐ Description of incident
- ☐ Reference to policy, procedure, or regulation applicable
- ☐ Explanation of significant or highly sensitive incident
- ☐ Analysis of how or why incident occurred

QIA Examples

Examples of a QIA include, but are not limited to:

- Tasking intelligence personnel to conduct activities that are not part of the Agency's approved mission, even if they have the technical capability.
- Intelligence personnel instructing non-intelligence personnel to conduct intelligence activities, or collect information not available through authorized collection techniques.
- Providing intelligence services and/or products without proper authorization.
- Collecting USPI, even through open source means, when it is not part of the unit's assigned mission.
- Of Note: Actions that are not inherently intelligence, such as fraud, waste and abuse, personal misconduct, and minor security violations or deviations are normally processed through Security channels.

S/HSM Examples

Examples of a S/HSM include, but are not limited to:

- Intelligence-related incidents involving congressional inquiries or investigations.
- Intelligence-related incidents that may result in adverse media coverage.
- The relief of an Intelligence activity leader for illegal conduct.
- Intelligence-related incidents that may impact foreign relations or foreign partners.
- A Naval Attaché or FAO will be or was relieved for cause.
- U.S. intelligence official meeting with and garnering official-like understandings with foreign officials without approval.

Command IO Inspections

DON components with intelligence or intelligence-related activities are subject to periodic IO inspections pursuant to DoD Manual (DoDM) 5240.01 and DoD Directive (DoDD) 5148.13. DoD SIOO has responsibility for inspecting all Military Departments/Components, Combatant Commands (CCMD), Combat Support Agencies (CSA) and other DoD intelligence organizations for IO compliance.

The DON has three primary types of inspections:

- Cognizant command IG “36-month” IO inspection
- DON SIOO (DUSN (I&S)) Staff Assistance Visit (SAV)
- Component federated inspections

In accordance with SECNAVINST 3820.3F, all commands and units with intelligence or intelligence-related activities will have IO compliance inspections at an interval of no more than 36 months.

The Naval Inspector General (NAVINSGEN) and Deputy Naval Inspector General of the Marine Corps (DNIGMC) are the official IO inspection arms of the DON.

The Intelligence Oversight Inspection Checklist can be found in SECNAVINST 3820.3F, enclosure 4 (see Appendix A), and includes five parts:

- Governance and management
- Reporting
- Training
- Inspections
- Investigations

Staff Assistance Visits are conducted by the DON SIOO to Service Components to enhance their awareness and understanding of intelligence oversight concepts and procedures, advise on how to create and implement a meaningful Intelligence Oversight program tailored to the mission of the Service Component, and provide specific

advice and guidance on intelligence oversight questions and concerns. SAVs can be requested by the Service Component or be directed in response to circumstances.

Echelon 3-4 Intelligence Oversight Responsibilities

DON Intelligence Oversight is a federated program. As such, the expectation is that Echelon 2 commands will inspect Echelon 3 commands and Echelon 3 commands will inspect Echelon 4 commands, and so on.

Echelon 2 commands, such as U.S. Fleet Forces Command (FFC) and U.S. Pacific Fleet, will generate a plan to inspect the IO programs of their subordinate Echelon 3 commands. For example, in the case of FFC, they would inspect Carrier Strike Group 4, U.S. Second Fleet, Naval Air Force Atlantic, etc. When required, Echelon 2 commands will direct subordinate commands to develop IO Compliance Programs.

If IO subject matter expertise is needed to conduct inspections at lower levels, the inspecting command should request subject matter expert support from their higher echelon.

This federated approach applies to quarterly reporting.

Best Practices

The best IO programs have involved leaders and legal advisors, tailored training programs, integrated planning, and established and active IO reporting and resolution procedures.

The following are notable best practices:

- The responsibility of the IOO should not be confused with security officer responsibilities.
- Training emphasizes that reporting QIAs is mandatory and that no adverse action will be taken against whistle-blowers.
- Establish and maintain records to document individual training, and to provide a mechanism to assure that those employees who miss training are trained at the earliest opportunity.
- Establish training processes that ensure personnel conducting intelligence-related support or personnel support receive additional training.
- Ensure the IOO maintains copies of EO 12333, DoD Directive 5240.01, DoD Manual 5240.01, DoD Directive 5148.13, and service or organization-specific implementing instructions.
- Use communication products (e.g. emails or bulletins) to supplement IO program awareness and education.

Appendix A: DON IO Inspection Checklist

IO INSPECTION CHECKLIST		
Inspected Organization:	Inspector(s):	Date:

References:
(a) E.O. 12333, as amended
(b) DoD Directive 5240.01 of 22 March 2019
(c) DoDM 5240.01, "Procedures Governing the Conduct of DoD Intelligence Activities," of 8 August 2016
(d) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," Incorporating Change 2, effective 26 April 2017
(e) DoD Directive 5148.13 of 26 April 2017
(f) SECNAVINST 3820.3F, "Oversight of Intelligence Activities within the Department of the Navy" dd mmm yyyy

Part 1: Governance and Management		
1	Does your organization have an IO Instruction, Standard Operating Procedure, or Manual? Remarks:	☐ Yes ☐ No
2	Does your organization have a designated Intelligence Oversight Officer (IOO)? - Is the IOO of appropriate grade and intelligence experience commensurate with their oversight responsibilities who has access to all organization intelligence and intelligence-related activities (including those protected by special access programs, alternative compensatory control measures, and other security compartments) and who has direct access to the organization commanding officer/director/head of report on intelligence oversight compliance? (DoD Directive 5148.13 para 2.4.h and SECNAVINST 3820.3F Enclosure (2) para 5.a Remarks:	☐ Yes ☐ No
3	Does your organization have a process for reviewing command intelligence activities and intelligence-related activities under the organization's authority, direction, and control to verify compliance with applicable federal law, E.O.'s, Presidential Directives, Intelligence Community Directives, DoD, and SECNAV issuances? - Does the process include a legal review when required, or appropriate? - Is process codified in an instruction or standard operating procedure, etc.? (DoD Directive 5148.13 para 2.4.a and SECNAVINST 3820.3F Enclosure (2) para 5.b Remarks:	☐ Yes ☐ No

4	Does your organization verify that all contracts involving intelligence or intelligence-related activities or supporting those efforts under DoD authorities requires personnel to report any QIA or S/HSM to appropriate government officials identified in the contract? (DoD Directive 5148.13 para 4.1.e and SECNAVINST 3820.3F Enclosure (2) para 5.i) Remarks:	☐ Yes ☐ No
5	Does your organization provide the DON organization legal counsel/SJA, GC/JAG/SJA to CMC, DUSN Intelligence IOO, and any IG of competent jurisdiction with access to any employee and with all information necessary to perform their IO oversight responsibilities, including information protected by SAP, alternative compensatory control measures, or other security compartmentalization? - Is the organization IG and legal counsel cleared to all programs/activities? (DoD Directive 5148.13 para 4.1.e and SECNAVINST 3820.3F Enclosure (2) para 5.i) Remarks:	☐ Yes ☐ No
6	Does your organization host or participate in shared repository (database)? - If so, does the shared repository contain USPI? - Is the shared repository with USPI done IAW DoDM 5240.01? - Is there an instruction, SOP or Manual for preventing a violation when storing or accessing the shared repository (database)? (DoDM 5240.01 para 3.1.b) Remarks:	☐ Yes ☐ No
	Part 2: Reporting	
7	Does your organization have a process to report S/HSM and QIA? - Immediately for S/HSM - Quarterly for QIA - Format in accordance with DoD SIOO and current DON template (DoD Directive 5148.13 para 4.1.d, 4.4.a, 4.4.b, and Figure 1 and SECNAVINST 3820.3F Enclosure (2) para 5.e and Enclosure (3)) Remarks:	☐ Yes ☐ No

8	Does your organization have a process to report any crimes involving any intelligence activity or intelligence-related activity to NCIS? (DoD Directive 5148.13 para 4.3.a(3) and SECNAVINST 3820.3F Enclosure (2) para 5.h) Remarks:	☐ Yes ☐ No
9	Does your organization submit quarterly IO reports? - Due no later than 5 calendar days after end of reporting quarter - Format in accordance with template - The Heads of DON organizations, including SYSCOMS, Program Executive Officers, and Heads of Naval Academic Institutions, that conduct intelligence or intelligence-related activities are responsible for submitting S/HSM, QIA, and Quarterly IO report to the DON Intelligence Oversight IO Official using the format in enclosure (3) (DoD Directive 5148.13 para 4.4.b, and Figure 1 and SECNAVINST 3820.3F Enclosure (2) para 5.b, or Enclosure (3)) Remarks:	☐ Yes ☐ No
	Part 3: Training	
10	Does your organization administer an IO training program that is appropriately tailored to mission requirements (initial and annual refresher)? - At a minimum, IO training will include:(1) Familiarity with the authorities and restrictions established in DoDD 5240.01, DoDM 5240.01, and other applicable Intelligence Community Directives and DoD issuances governing applicable intelligence activities. (2) Responsibilities of DoD personnel and DoD contractor personnel for reporting QIAs and S/HSMs - What is the process for tracking and documenting? - Does all senior leadership, with cognizance over intelligence or intelligence-related activities, review IO training? (DoD Directive 5148.13 para 2.4.c and SECNAVINST 3820.3F Enclosure (2) para 5.c) Remarks:	☐ Yes ☐ No
11	Do individuals at the organization understand: - What constitutes a S/HSM, QIA, and USPI? - S/HSM and QIA reporting responsibilities (report immediately to their chain of command or supervisors) - Restriction established in DoDD 5240.01 and DoDM 5240.01(DoD Directive 5148.13 para 2.4.c, 4.1.d and SECNAVINST 3820.3F Enclosure (2) para 5.d) This question is used to determine effectiveness of intelligence oversight training. Remarks:	☐ Yes ☐ No

Part 4: Inspections		
12	Does your cognizant Command IG conduct IO inspections on all components, units, and elements in or under your command at an interval of no greater than once every 36 months, with appropriate follow-up/"spot checks" or assistance between inspections as deemed necessary? (DoD Directive 5148.13 para 4.1.b through d and SECNAVINST 3820.3F Enclosure (2) para 5.f) Remarks:	☐ Yes ☐ No
Part 5: Investigations		
13	Does your cognizant Command IG conduct IO investigations into alleged QIAs and S/HSMs to the extent necessary to determine that facts and to assess whether the activity is legal and consistent with applicable policies? - Investigations will require a written report that includes a description of the incident and a determination of whether the allegation was substantiated. If the allegation is substantiated, does the report include findings of fact, assessment of the cause, and the recommended remedial action to prevent recurrence? - How are they referred to IG? (DoD Directive 5148.13 para 4.2.a and SECNAVINST 3820.3F Enclosure (2) para 5.g) Remarks:	☐ Yes ☐ No

Additional Notes:

Inspecting Official (Print Name, Title, Phone)	Inspecting Official's Signature

NOTES:

This Handbook is intended to provide an overview of IO policies and to guide readers to appropriate references.

For additional assistance, contact your higher headquarters IO professional.

For training briefs, templates, and courses, or for questions about this Handbook, contact the DUSN I&S, Intelligence Directorate at 703-693-7319 or TS DVTC 912-0764, or email DONIntelOversight@us.navy.mil or DONIOO.fct@navy.smil.mil

Deputy Under Secretary of the Navy (Intelligence and Security)

1200 Navy Pentagon
Washington, DC 20350-1200
https://www.navy.mil/DUSN-Intelligence-and-Security/