



Command Policy

INTELLIGENCE OVERSIGHT PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available electronically on the USTRANSCOM electronic library.

RELEASABILITY: There are no releasability restrictions on this publication

OPR: TCIG
Supersedes: USTRANSCOMI 90-4, 24 June 2004

Approved By: TCDC (VADM Mark D. Harnitchek)
Pages: 7
Distribution: e-Publishing

Authority for this Instruction is Executive Order 12333, United States (US) Intelligence Activities. It implements Department of Defense (DOD) 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components that Affect US Persons*. This Instruction reaffirms the United States Transportation Command (USTRANSCOM) Intelligence Oversight Program. It ensures that the activities (collecting, retaining, and disseminating foreign intelligence and counterintelligence) of USTRANSCOM intelligence staff are conducted in accordance with applicable guidance. The purpose of these procedures is to enable the Intelligence staff to effectively carry out their authorized functions in a manner that protects the constitutional rights and privacy of US persons. It applies to all personnel assigned or attached to USTRANSCOM, including the Joint Transportation Reserve Unit. This Instruction is subject to the Paperwork Reduction Act of 1995. Refer to USTRANSCOMI 33-39, *Information Collections and Report Management Program*, for guidance. Refer recommended changes and questions about this publication to the office of primary responsibility using Air Force Form 847, *Recommendation for Change of Publication*. Ensure that all records created as a result of processes prescribed in this Instruction are maintained in accordance with USTRANSCOM Instruction 33-32, *USTRANSCOM Records Management*.

SUMMARY OF REVISIONS

Updates DOD, and Joint Chiefs of Staff (JCS) references to reflect current intelligence oversight procedures along with current terminology. This Instruction has been revised in its entirety, asterisks will not be used to identify revised material.

1. References and Supporting Information: Publications referenced in this Instruction are listed in Attachment 1.

2. Policy:

2.1. Intelligence oversight is broader in scope than the simple protection of US citizens' rights to privacy or intrusion from intelligence gathering agencies. It includes the assurance that the measures used to acquire intelligence information respond to the legitimate needs of the US

Government and are employed in a manner consistent with the legal and constitutional rights of US persons. USTRANSCOM intelligence activities that affect US persons will be conducted within constraints imposed by the referenced regulations and directives.

2.2. USTRANSCOM Directorate of Intelligence (TCJ2) personnel will report to the appropriate authorities all intelligence activities that violate Federal laws and national directives.

2.3. No adverse action will be taken against any member who reports violations of this policy.

2.4. Requests for exceptions to established DOD intelligence oversight policies may be made in writing to the Assistant to the Secretary of Defense for Intelligence Oversight through appropriate USTRANSCOM and Joint Staff channels.

2.5. No USTRANSCOM intelligence tasking, whether or not concerning a US person, will be initiated unless it is within the assigned function of the intelligence component concerned, and has been approved by proper authority, including legal or other review as may be prescribed or appropriate under the circumstances.

3. Responsibilities:

3.1. USTRANSCOM Inspector General (TCIG) will:

3.1.1. Provide oversight of intelligence activities for USTRANSCOM in accordance with Federal and other appropriate laws, Executive Orders, and other referenced directives and instructions.

3.1.2. Conduct selected assessments and compliance inspections of joint intelligence activities, including the authorized collection, production, exploitation, surveillance, analysis, reporting, and dissemination activities, to determine if USTRANSCOM intelligence organizations are involved in any questionable activities which violate the constitutional rights of individuals. Assessments and compliance inspections within USTRANSCOM will be conducted semiannually. The guideline of these assessments will be the checklist at Attachment 2.

3.1.3. Review existing procedures for reporting questionable activities and ensure that personnel are aware of their responsibilities to report such activities.

3.1.4. Coordinate with USTRANSCOM Staff Judge Advocate (TCJA) any investigation of questionable intelligence activities to determine whether the activity is legal and consistent with applicable policy and/or laws.

3.1.5. Report any questionable intelligence activities without delay. Additionally, consolidate USTRANSCOM command reports on intelligence oversight activities and submit a quarterly report to the Assistant to the Secretary of Defense for Intelligence Oversight, through the Joint Chiefs of Staff Inspector General Office.

3.2. TCJA will:

- 3.2.1.** Review all USTRANSCOM intelligence activities involving collection, production, exploitation, surveillance, analysis, reporting, and dissemination of intelligence to ascertain consistency with law and policy.
- 3.2.2.** Provide direct legal support to USTRANSCOM operations and intelligence organizations concerning intelligence oversight issues, to include but not limited to the following:
- 3.2.2.1.** Collection of information on US persons by intelligence organizations.
- 3.2.2.2.** Advice by intelligence personnel to Federal, State, or local law enforcement officials.
- 3.2.2.3.** Dissemination of information collected on individuals without their consent.
- 3.2.2.4.** Retention of information about individuals, even if on a temporary basis, while assessing criteria for permanent retention.
- 3.2.2.5.** Airborne imagery in support of counter-narcotics operations and overhead imagery from reconnaissance not directed at specific persons.
- 3.2.2.6.** Human resources intelligence policies and restrictions.
- 3.2.2.7.** Electronic surveillance procedures, restrictions, and authorization.
- 3.2.2.8.** Counterterrorism information collected about individuals to protect persons or organizations which are targets, victims, or hostages of international terrorist organizations.
- 3.2.3.** Make legal counsel support available to assist in familiarizing and maintaining training for intelligence personnel regarding their responsibilities relating to the conduct of intelligence operations and the rights of US persons.
- 3.2.4.** Ensure the availability of legal counsel in support of inquiries or investigations regarding intelligence oversight matters.
- 3.2.5.** Participate with TCIG in conducting inspections and evaluations. Provide input to the quarterly report of intelligence activities within USTRANSCOM control.
- 3.2.6.** Coordinate with TCIG on discovering and reporting questionable activities. Determine the legality and propriety of questionable activities.
- 3.2.7.** Report all questionable activities of a serious nature to the DOD General Counsel, through the Joint Chiefs of Staff Legal Advisor, without delay.
- 3.2.8.** Maintain a library of Federal laws, Executive Orders, DOD directives, regulations, policy statements, and other references applicable to the USTRANSCOM Intelligence Oversight Program.

3.3. Intelligence Directorate (TCJ2) and Joint Transportation Reserve Unit will:

3.3.1. Ensure that all personnel are trained initially upon assignment and annually thereafter regarding Intelligence Oversight rules and responsibilities. New personnel must provide proof of training from previously assigned unit or receive training from TCJ2.

3.3.2. Ensure that procedures exist for reporting questionable activities and that assigned personnel are aware of their responsibility to report such activities.

3.3.3. Conduct or provide support for the conduct of intelligence gathering activities only with proper authorization and in accordance with the constitutional rights and privacy of US persons.

3.3.4. Ensure that all intelligence activities which raise issues of legality or propriety are given appropriate legal review prior to implementation or as soon as identified.

MARK D. HARNITCHEK
Vice Admiral, U.S. Navy
Deputy Commander

Attachments:

1. References and Supporting Information
2. Inspection Checklist

ATTACHMENT 1

REFERENCES AND SUPPORTING INFORMATION

Executive Order (EO) 12333, 4 Dec 81, *United States Intelligence Activities*
Department of Defense Directive, DODD 5240.01, *DOD Intelligence Activities*
Department of Defense, DOD 5240.1-R, *Procedures Governing the Activities of DOD
Intelligence Components that Affect United States (US) Persons*
DODD 5525.5, *DOD Cooperation with Civilian Law Enforcement Officials*
Chairman, Joint Chiefs of Staff, CJCSI 5901.01B, *Conduct of Inspections, Investigations and
Intelligence Oversight*
DODD 5148.11, *Assistant to the Secretary of Defense for Intelligence Oversight*

ATTACHMENT 2

USTRANSCOM Intelligence Oversight (IO) Inspection Guidance

Inspectors and IO Program Managers will follow this checklist when assessing the adequacy of IO programs. In order to receive a Satisfactory rating, the unit must Pass all critical items. The unit will receive a Marginal rating if one critical item is failed. If more than one critical item is failed, the unit will receive an Unsatisfactory rating. Passing all items will result in a Superior rating. Passing 5/8 non-critical items will result in an Excellent rating.

	Critical	Non-Critical	Pass	Fail
1. Administrative Criteria.				
1.1. Are the primary and alternate intelligence oversight monitors appointed, in writing, and made known to the unit via poster or appointment letter? (If failed, unit will update paperwork within 10 days)		X	<input type="checkbox"/>	<input type="checkbox"/>
1.2. Are copies of Executive Order 12333, DODD 5240.1, DOD 5240.1-R, CJCSI 5901.01B, DTM 08-052, and, USTRANSCOMI 90-4 available in hard or electronic copy? (If failed, correct on spot and show where electronic copies are available)		X	<input type="checkbox"/>	<input type="checkbox"/>
1.3. Did at least 80% of unit personnel receive training within 60 days of reporting for duty? (If failed, corrective actions will be put in place within 30 days.)	X		<input type="checkbox"/>	<input type="checkbox"/>
1.4. Did at least 80% of the unit personnel receive recurring training within the last year? (If failed, unit will bring training percentage to 80% within 15 days and accomplish 100% recurring training within 60 days.)	X		<input type="checkbox"/>	<input type="checkbox"/>
1.5. Are initial and annual training lesson plans current and available? (If unit fails, the lesson plan must be updated and re-inspected within 30 days)	X		<input type="checkbox"/>	<input type="checkbox"/>
2. Management Criteria.				
2.1. Are at least 80% of Senior Managers interviewed aware of IO requirements and limitations? (If failed, Senior Managers receive remedial training within 60 days)	X		<input type="checkbox"/>	<input type="checkbox"/>
2.2. Has a periodic screening of intelligence holdings occurred in the last 6 months? (If failed, screening will be accomplished, appropriate actions taken, and the results and actions forwarded to TCIG and TCJA within 30 days of inspection)		X	<input type="checkbox"/>	<input type="checkbox"/>
2.3. Would existing oversight processes identify any unauthorized searches for management to act upon? (If failed, corrective actions in place within 30 days)		X	<input type="checkbox"/>	<input type="checkbox"/>

2.4 Would existing oversight processes identify any unauthorized surveillance or monitoring for management to act upon? (If failed, corrective actions in place within 30 days)		X	<input type="checkbox"/>	<input type="checkbox"/>
2.5 Is information on US Persons collected or stored over 90 days without a legal opinion stating it is IAW DOD guidance? (If failed, corrective action in place within 90 days)		X	<input type="checkbox"/>	<input type="checkbox"/>
3. Unit Member Criteria (If unit fails any unit member measures, personnel will accomplish recurring training within 60 days.)				
3.1. Can 80% of interviewed personnel name the IO monitor or alternate?		X	<input type="checkbox"/>	<input type="checkbox"/>
3.2. Can 80% of unit members interviewed explain how to get a copy of the guidance listed in Section 1.2 above?		X	<input type="checkbox"/>	<input type="checkbox"/>
3.3. Do 80% of unit members interviewed include a broader perspective of "US Persons" than just US Citizens?	X		<input type="checkbox"/>	<input type="checkbox"/>
3.4. Can 80% of unit personnel interviewed explain the circumstances under which intelligence can be collected, retained, and disseminated on US persons?	X		<input type="checkbox"/>	<input type="checkbox"/>
3.5. Can 80% of unit personnel describe the IO limitations in the collection of intelligence on US persons by electronic or physical surveillance?	X		<input type="checkbox"/>	<input type="checkbox"/>
3.6. Can 80% of unit personnel interviewed relate the general restrictions on providing intelligence support to law enforcement agencies?	X		<input type="checkbox"/>	<input type="checkbox"/>
3.7. Can 80% of unit personnel interviewed describe the circumstances under which they must report "questionable activities" conducted by intelligence components that constitute possible violations of law, directive, or policy and to whom they are supposed to report it?	X		<input type="checkbox"/>	<input type="checkbox"/>