DEPARTMENTS OF THE ARMY AND THE AIR FORCE
National Guard Bureau
Washington, DC 20310-2500
15 September 1995

NGR 20-10/ANGI 14-101

Assistance, Inspections, Investigations, and Followup

INSPECTOR GENERAL INTELLIGENCE OVERSIGHT PROCEDURES

Summary. This regulation provides guidance for National Guard Inspectors General (IG) to implement oversight of intelligence activities.

Applicability. This regulation addresses procedures that apply to all Army and Air National Guard units, activities and staffs, to include the National Guard Bureau (NGB), when conducting intelligence activities. It is intended for use by State Inspectors General to assist in their execution of AR 20-1 Intelligence Oversight (IO) responsibilities.

Impact on New Manning System. This regulation does not contain information that affects the new manning system.

Internal Control Systems. This regulation is not subject to the requirement of AR 11-2.

Supplementation. Supplementation of this regulation is prohibited without prior approval from National Guard Bureau-Inspector General (NGB-IG), Washington, DC 20310-2500.

Interim changes. Interim changes to this regulation are not official unless they are authenticated by the Chief, Administrative Services. Users will destroy interim changes on their expiration dates unless sooner superseded or rescinded.

Suggested Improvements. The proponent agency of this regulation is the National Guard Bureau (NGB-IG). Users are invited to send comments and suggested improvements on DA form 2026 (Recommended Changes to Publications and Blank Forms) directly to Chief, National Guard Bureau, **ATTN:** Office of the Inspector General (NGB-IGI), The Pentagon, Rm. 2E379, Washington, DC 20310-2500.

Contents *(Listed by paragraph number)*

Chapter 1
Introduction — **Para**
Purpose — 1-1
References — 1-2
Explanation of abbreviations and terms — 1-3
AR 381-10 Extract — 1-4
Responsibilities — 1-5

Chapter 2
General
Executive Order (EO 12333) — 2-1
Departmental Regulations — 2-2
National Guard Regulations — 2-3
Questionable Activities — 2-4

Chapter 3
Guidance
Detailed Guidance — 3-1
Reporting Procedures — 3-2
Intelligence Training and Operations — 3-3
Communications and Operations Security — 3-4
Public Affairs — 3-5
Legal Documentation for Counterdrug Activities — 3-6

Appendixes
A. References
B. Extracts from AR 381-10
C. Intelligence Oversight Criteria

Glossary

Chapter 1
Introduction

1-1. Purpose
This regulation prescribes the policies, procedures, responsibilities, and guidance for National Guard Inspectors General to implement IG oversight of intelligence activities.

1-2. References
Required and related publications are listed in **appendix A.**

1-3. Explanation of abbreviations and terms
Abbreviations and special terms used in this regulation are explained in the **glossary.**

1-4. AR 381-10 Extract
Procedures Governing the Activities of Intelligence Components that Affect United States Persons are listed in **appendix B.**

1-5. Responsibilities
a. NGB Inspector General (NGB-IG). The NGB-IG Intelligence Oversight Officer will provide IG oversight of all intelligence, intelligence-related, counterintelligence (CI), military support to civilian authorities (MS), and counterdrug support program (CD) information gathering activities within the National Guard (NG). This generally includes oversight of the

National Guard Bureau, the Office of the Chief, the Army and Air National Guard Directorates, and the 54 states and territories. NGB-IG Intelligence Oversight Officer specific functions include--

(1) Assist State IGs in execution of their AR 20-1 Intelligence Oversight responsibilities.

(2) Inspect NG components that engage in intelligence and counterdrug activities, as directed by CNGB, assuring compliance with law, Department of Defense (DoD), Departmental and National Guard requirements.

(3) Monitor investigations and inspections by DoD components and other government agencies of intelligence and counterdrug activities.

(4) Serve as the NGB point of contact in the IO arena.

(5) Review Army/Air Directorate proponent policies and recommend improvements.

(6) Liaison with the Secretary of the Army Inspector General, Intelligence Oversight Division (SAIG-IO), The Secretary of the Air Force Inspector General, Special Investigations Directorate, and with other agencies as required.

(7) Responsible for Intelligence Oversight inquires and investigations of possible violations reported by National Guard personnel.

b. State Inspectors General. State Inspectors General, as part of their oversight responsibilities, will--

(1) Inspect intelligence functions and activities within their states as directed by the Adjutant General (TAG).

(2) Determine what organizations, staffs, or offices are used for intelligence purposes, and oversee compliance with appropriate directives. (Refer to AR 20-1, para 1-4b(7).)

(3) Review, in consultation with the Staff Judge Advocate (SJA), the propriety of planned and on-going information collection and CD activities.

(4) Determine if intelligence components, or other elements performing intelligence-type activities are involved in "questionable activities."

(5) Ensure that procedures exist within organizations, staffs, or offices used for intelligence purposes for the reporting of questionable activities, and that personnel of such components are aware of their responsibilities to report such activities.

(6) Report all "questionable activities" to the NGB-IGI, NLT 5 days after discovery.

(7) Forward copies of intelligence related findings/inspection reports to CNGB, ATTN: NGB-IGI.

(8) Coordinate with the SJA for interpretation of state law and applicable directives as they relate to local information collection activities. Unresolved questions should be forwarded to NGB-IGI for coordination, resolution, or additional legal review.

Chapter 2
General

2-1. Executive Order (EO) 12333

EO 12333 governs the conduct of intelligence activities for agencies within the Intelligence Community (Refer to EO 12333, Part 1, para 1.4 and Part 3, para 3.4 (f)). It provides implementing instructions and attempts to strike a balance between the rights of US persons and the government's need for essential information. The order attempts to ensure--

a. Protection of an individual's constitutional rights and privacy.

b. Collection of essential authorized information by the least intrusive means.

c. Dissemination of information limited to lawful government purposes.

2-2. Departmental Regulations

EO 12333 procedures, agreed upon by the Attorney General and Secretary of Defense, have been promulgated within DoD Directive 5240.1 and DoD Regulation 5240.1-R. The Army has implemented the DoD directives through AR 381-10. Likewise, Air Force implementation is through AFI 14-104.

2-3. National Guard Regulations

The NGB has published a joint regulation, NGR (AR) 381-10/(AF) 200-19 (now AFI 14-104) that supplements AR 381-10 and AFI 14-104 by establishing the requirement for an Intelligence Oversight program in all National Guard intelligence activities. The procedures apply to--

a. Army and Air National Guard units, activities, staffs, and personnel, to include the Office of the Chief, National Guard Bureau when performing federal intelligence duties in a Title 10 or Title 32 status, or engaging in intelligence activities directly related to a federal mission or duty.

b. This includes, but is not limited to, MS and CD activities.

2-4. Questionable Activities

The term "questionable activity" has not been succinctly defined. The Executive Order, Department of Defense Directives, and service regulations describe "questionable activities" as any conduct that constitutes, or is related to, an intelligence activity that **may** violate law, any Executive Order, Presidential directive, applicable DoD policy, AFR 200-19 (now AFI 14-104), and AR 381-10 (emphasis added). No attempt is made to either expand or restrict this definition within this regulation. State IGs are encouraged to report what they perceive to be "questionable activity" and seek assistance from NGB-IGI when appropriate.

Chapter 3
Guidance

3-1. Detailed Guidance

NG organizations performing intelligence activities should have an Intelligence Oversight Program. Most established intelligence units have such a program. Many newly formed activities may not. The Intelli-

gence Oversight Program should be included within AR 1-201, Organizational Inspection Programs (OIP). The IO programs should address the following:

a. Each organization will have additional duty orders on file that assigns primary and alternate IO monitors responsible for its program. Unit personnel should know the identity of those responsible and should be aware of the restrictions placed on their organization, as well as the purpose of IO. Personnel will receive oversight briefings upon joining the unit and refresher briefings annually. Briefings will be included in the unit commander's Yearly Training Guidance and Calendar.

b. AR 381-10, Army Intelligence Activities and AR 380-13, Acquisition and Storage of Information Concerning Not Affiliated Persons and Organizations prohibit US military personnel and agencies from both active (physical deployment of surveillance personnel) and passive (police reports, open-source material (OSINT)) collection, and storage and distribution of information on US persons and organizations. As an example, civil disturbance information developed or acquired during an authorized period of acquisition, reporting or processing activities must be destroyed within 60 days after the termination of the civil disturbance.

c. Many units maintain an Intelligence Oversight Policy Book. This book should contain a copy of the applicable regulations/SOPs, and training materials. Documentation should record signatures and dates personnel receive oversight briefings.

d. **Appendix C** is provided as a guide for conducting IG assessments and inspections.

e. Query personnel within an intelligence organization to confirm whether they can identify regulations governing reporting procedures on "questionable activities" and the identity of the Intelligence Oversight Officer.

f. The National Security Agency (NSA) is the only organization which can authorize real-world SIGINT collection activities. Under no circumstances can units perform real-world SIGINT collection activities independently, or under the direction of a Governor, in support of state missions.

g. Units involved in Signals Intelligence (SIGINT) should be aware of the United States Signals Intelligence Directives (USSIDs) 18 (S), 1600NG (ARNG) (S), and 3500NG (ANG) (S). These regulations dictate performance boundaries within SIGINT training and operations. They are stored in the Sensitive Compartmented Information Facility (SCIF) at the supporting Special Security Office (SSO). A Top Secret (TS) clearance with Sensitive Compartmented Information (SCI) access is required to view these documents.

h. Access to Sensitive Compartmented Information requires a "billet" (a formal authorization for SCI access). It also requires a single scope background investigation (SSBI) which may take six months or longer to obtain. One person in the State IG office will have this clearance/access if the state has units performing SIGINT activities. Direct questions to your State Security Manager or supporting SSO on processing TS clearances and billets for SCI access. NGB-IGI can provide assistance if necessary.

i. State IGs will verify that unit commanders and program managers ensure that assigned personnel understand applicable AR 381-10 procedures.

j. The following types of units/programs should have an IO Program.

(1) Brigade, Division and State Area Command (STARC) G2/S2 staffs (ARNG).

(2) Divisional MI Battalions and Divisional MI Battalions (Cadre) (ARNG).

(3) Military Intelligence Brigades/Battalions (Linguist) (ARNG).

(4) Special Forces Units/Special Operations Groups/Long Range Surveillance Units (ARNG).

(5) Counterdrug Programs, Coordinators, and staffs.

(6) Intelligence Squadrons (ANG) and Reconnaissance Groups and Squadrons (ANG).

(7) Enhanced Brigade and Armored Cavalry Regiment Direct Support Companies (ARNG).

(8) Fighter, Interceptor, and Airlift Unit Intelligence Staffs (ANG).

(9) Counterintelligence Detachments (ARNG).

3-2. Reporting Procedures

Established AR 381-10 channels for reporting "questionable activities" are numerous and fragmented. For simplicity, NG organizations will report "questionable activities" through established reporting channels to the State IG. IGs will forward such reports to NGB-IG within 5 days of receipt. Reports will include the following information:

a. Description of the nature of the "questionable activity."

b. Date, Time, and location of occurrence.

c. Individual or unit responsible for the "questionable activity."

d. Summary of the incident including references to particular portions of AR 381-10.

e. Status of the investigation regarding the incident.

State IGs will submit a quarterly report to NGB-IG describing any actions taken relative to "questionable activities" previously reported, significant oversight activity accomplished during the quarter, along with any suggestions for improvement within the oversight system. Reports are due within five days after the close of each quarter. Negative reports are required, unless otherwise directed. Requests for exception to these reporting requirements will be submitted to NGB-IGI.

3-3 Intelligence Training and Operations

a. Counterintelligence involves gathering information and performing activities to protect against espionage, other intelligence activities, sabotage or assassinations conducted for or on behalf of foreign powers, organizations, persons, or international terrorist activities.

(1) Jurisdiction for domestic counterintelligence activity lies with the Federal Bureau of Investigation. This delineation of responsibility is based on "The Agreement Between the Deputy Secretary of Defense and Attorney General, dated April 5, 1979". An extract of this document is found within AR 381-10, appendix B.

(2) The Army Central Control Office (ACCO) exercises technical control, review, coordination and oversight of CI controlled activities. It is the only Army organization which can authorize CI activities within CONUS. (Refer to AR 381-20, Chapter 3, para 3-2.)

(3) National Guard Counterintelligence agents can become involved in CI activities only in a Title 10 status or in active service to the U.S. Government. The ARNG has no independent authority to engage in real-world CI activity. However, CI units may conduct training during Inactive Duty Training (IDT) and Annual Training (AT).

(4) Army National Guard CI training is encouraged during IDT and AT periods. However, local Law Enforcement Agencies (LEA) must be informed if these activities occur in a public area. The "targets" of this training cannot be private citizens unless they are role-playing NG members who have given their prior consent. An example might include a field exercise where CI agents trail "suspects" to gather information. Training relationships with active duty CI organizations is encouraged to enhance training opportunities, subject to the same limitations.

(5) Air National Guard units/activities are not authorized to engage in independent domestic CI activity, including training. (Refer to AFI 71-101, Chapter 3, para 3.1.1.)

b. CD activities are not addressed in either DoD 5240.1-R or AR 381-10. However, at least three activities could fall under one of the procedures in these regulations: Electronic Surveillance (Procedure 5); Concealed Monitoring (Procedure 6); and Physical Searches (Procedure 7). DoD 5240.1-R, AR 381-10 and AFI 14-104 will be reviewed to determine if other procedures apply.

c. Counterdrug activities providing intelligence data derived from translation of tapes recorded by federal, state, or local law enforcement agencies will not be retained in NG facilities. Tapes may be held until translated. Once translated, all associated materials will be immediately returned to the appropriate agency within two working days.

d. Imagery Intelligence (IMINT) includes photographic, infrared, radar, and electro-optic images captured using ground or aerial based systems. In the past, these systems were confined to terrain mapping or used in military exercises. Today, they also may be used to support CD activities. These systems must not be targeted against US persons.

3-4. Communications and Operations Security

a. Safety of personnel and facilities is paramount. Operations Security (OPSEC) is necessary to ensure personnel and facilities are protected.

b. When applicable, secure mode communication is recommended. Type I STU-III terminals cannot be given to state LEAs; however, Type II terminals are authorized for issue. State level STU III users (i.e., Plans, Operations, and Training Officer (POTO) or Directorate of Information Management (DOIM)) comply with guidance provided by NGB-AIS.

c. State IGs visiting CD field activities should review instructions issued toward protecting sensitive information and media relations. Information does not necessarily have to be classified to be sensitive. Sensitive CD plans and activities should be marked "For Official Use Only" and should be protected IAW AR 25-55 (Freedom of Information Act (FOIA)). Documents being released to an LEA should contain the caveat "This document contains information EXEMPT FROM MANDATORY DISCLOSURE under the FOIA". LEAs should be advised of information sensitivity. Information should be restricted to a "need-to-know" basis.

d. The FOIA may be used by the media, private individuals, and anyone outside NG/LEA channels to obtain intelligence operational data. AR 340-17 (Release of Information and Records from Army Files), paragraph 1- 508e directs referring requests to the originating component. For SIGINT activities, the NSA is the only authority that determines whether information is releasable.

3-5. Public Affairs

a. Media and public interest in IG activities can be intense and immediate. Participants in any IG activity should coordinate with state Public Affairs Officers as one of the first events of any IG action.

b. Personnel should refer media inquires and other requests for information from outside of NG / LEA channels to the state PAO. The supported LEA should have the lead concerning public affairs and make the final determination concerning release of information to the public in coordination with the state PAO. See NGR (AR) 500-2/ANGI 10-801, paragraph 2-10.

c. The Public Affairs Officer (PAO) should consult with CD Coordinators to determine if Operations Security (OPSEC) issues exist within news releases.

3-6. Legal Documentation for Counterdrug Activities

a. Supported LEAs are responsible for obtaining the legal authorization required to permit information gathering. A Memorandum of Understanding (MOU) will be on file stating this responsibility falls upon the

supported LEA. This MOU will remain on file for a minimum of two years following the completion of Counterdrug support to the related LEA.

b. Counterdrug Support Plans will be reviewed to ensure it includes a State Attorney General certification that the plan has been reviewed and is legally permissible under state law.

APPENDIX A
References

Section I
Required Publications

AFI 14-104
Conduct of Intelligence Activities.

AR 20-1
Inspector General Activities and Procedures. (Cited in para 1-4b (7).)

AR 380-13
Acquisition and Storage of Information Concerning Non-affiliated Persons and Organizations.

AR 381-10
U. S. Army Intelligence Activities.

AR 381-12
Subversion and Espionage Directed Against US Army (SAEDA).

AR 381-20
The Army Counterintelligence Program. (Cited in Chapter 3, para 3-2.)

AR 500-51
Support to Civilian Law Enforcement.

DoD 5240.1
DoD Intelligence Activities.

DoD 5240.1-R
Procedures Governing the Activities of DoD Intelligence Components that Affect U. S. Persons.

NGR (AR) 381-10/AFI 14-104
Conduct of Intelligence Activities.

NGR (AR) 500-1/NGR (AF) 55-5
Military Support to Civil Authorities.

NGR (AR) 500-2/ANGI 10-801
National Guard Counterdrug Support.

USSIDs
U. S. Signals Intelligence Directives.

Section II
Related Publications
A related publication is merely a source of additional information. The user does not have to read it to understand this regulation.

AFI 90-201
Inspector General Activities.

AR 25-55
Freedom of Information Act.

AR 340-17
Release of Information and Records from Army Files.

AR 381-1
Control of Dissemination of Intelligence Information.

EO 12333
Executive Order No. 12333 of United States Intelligence Activities.

NG PAM (AR) 500-2/ANG PAM 10-801
National Guard Counterdrug Coordinator's Handbook.

APPENDIX B
Extract of AR 381-10, Procedures Governing the Activities of Intelligence Components That Affect United States Persons

PROCEDURE 1
Governs general provisions. The purpose of these procedures is to enable intelligence activities to effectively carry out their authorized functions while ensuring their activities that affect United States Persons are carried out in a manner that protects the constitutional rights and privacy of such persons.

For activities in support of the Counterdrug Program, this means the National Guard has no independent authority to collect, process, retain, or distribute information.

PROCEDURE 2
Describes the categories of collectable information. This procedure sets forth general criteria governing the means used to collect such information. Information must fall within one of the following categories:

Category 1	Information obtained with consent.
Category 2	Publicly available information.
Category 3	Foreign intelligence information.
Category 4	Counterintelligence information.
Category 5	Information pertaining to potential sources of assistance to intelligence activities (For the purpose of determining their suitability and credibility).
Category 6	Information concerning the protection of intelligence sources and methods.
Category 7	Physical Security.
Category 8	Personnel Security Investigative Information.
Category 9	Communication Security.
Category 10	International Narcotics Activities.
Category 11	Information required to protect the safety of any person or organization.

Category 12 Overhead reconnaissance not directed at specific United States Persons.
Category 13 Administrative purposes.

Although Category 4 references counterintelligence operations, no circumstances exist for National Guard units/personnel to engage in domestic CI activities in a Title 32 status. Supporting an active component unit would allow Guardmembers to engage in this activity.

PROCEDURE 3
Governs the kinds of information about United States persons that may knowingly be retained by a DoD intelligence component without the consent of the person whom the information concerns, except solely for administrative purposes. The criteria for retention includes:

a. Information collected under PROCEDURE 2.

b. Information acquired incidentally.

c. Information relating to functions of other US government agencies.

d. Temporary retention.

e. Retention of other information.

PROCEDURE 4
Governs the kinds of information about United States persons that may be disseminated, without their consent, outside the intelligence activity that collected and retained the information. Distribution to federal, state, and local law enforcement agencies is allowed if the information relates to involvement in illegal activities. Information must be related to the performance of a lawful government function of the agency if the prospective recipient is a non-law enforcement, non-intelligence agency of the federal government.

PROCEDURE 5
Governs intercept, retention, and dissemination of communications concerning US persons elements of the United States SIGINT system. Activities within the United States are limited to foreign intelligence and counterintelligence purposes. These activities are governed by the United States Signals Intelligence Directives (USSIDs) 1600NG and 18.

PROCEDURE 6
Applies to concealed monitoring for foreign intelligence and counterintelligence purposes, **where the subject does not have a reasonable expectation of privacy and no warrant would be required for law enforcement purposes.** This includes visual surveillance, targeting by electronic, photographic, optical, electro-optical, infrared, other mechanical devices, airborne and ground-based systems.

For details concerning this procedure refer to AR 381-10 (emphasis added).

PROCEDURE 7
Applies to physical searches. Guardmembers are not authorized to conduct physical searches, except Counterdrug missions involving cargo inspections outlined in NGR (AR) 500-2/(AF) 55-6.

PROCEDURES 8, 9, 10, 11, 12, and 13
Guardmembers are not authorized to conduct activities described in these procedures.

PROCEDURE 14
Describes responsibilities to conduct intelligence and information collection activities IAW Executive Order 12333. Familiarization with the following restrictions are required:

a. Applicable portions of Procedures 1 through 4.

b. A summary of other procedures that pertain to collection techniques which are, or may be employed by the organization/activity concerned; and

c. A statement of individual responsibility under Procedure 15.

PROCEDURE 15
Provides for the identification, investigation, and reporting "questionable activities." IGs should review this procedure entirely to ensure organizations/ activities/units and personnel understand and comply with this procedure (emphasis placed on Special Operations forces, intelligence units with CI and SIGINT capability, and Counterdrug programs is recommended).

APPENDIX C
INTELLIGENCE OVERSIGHT CRITERIA

Related Questions

C-1. Does the organization have additional duty orders on file appointing primary and alternate Intelligence Oversight (IO) monitors?

C-2. Do unit personnel, performing intelligence duties, know the identity of the IO monitors?

C-3. Does the unit/activity maintain a copy of the applicable regulations noted below? (ARNG units are not required to maintain copies of Air Force Instruction (AFI)).

DoD 5240.1	DoD Intelligence Activities
DoD 5240.1-R	Procedures Governing the Activities of DoD Intelligence Components
AR 381-10	U. S. Army Intelligence Activities
AR 381-20	U.S. Army Counterintelligence Activities
NGR (AR) 381-10/ AFI 14-104	Conduct of Intelligence Activities
NGR(AR) 500-2/ANGI 10-801	National Guard Counterdrug Support

AFI 14-104	Conduct of Intelligence Activities
AFI 14-105	Intelligence Mission and Responsibilities
AFI 90-201	Inspector General Activities

C-4. Has a unit SOP been established to ensure members do not engage in unauthorized intelligence activities? (Only a very basic SOP is needed. It should parallel the requirements of NGR (AR)381-10/(AF)200-19 (now AFI 14-104) and identify the IO monitor.)

C-5. Do personnel have access to the SOP and the regulations?

C-6. Does the organization collect, analyze, retain, or disseminate any information concerning U.S. persons? If so, is it for valid military support to civil authority missions, support of counterdrug missions, or other properly authorized missions? Is there a possible criminal threat? (These are the only three circumstances under which it could be authorized.)

C-7. Where is the activity in question 6 taking place? Within a National Guard facility? (No activity, which could potentially result in use of information on U.S. persons, may be performed in NG facilities. Tapes recorded by LEAs may be temporarily retained until translated, and then must be immediately turned over to the supported LEA. No further analysis beyond simple translation may be performed within NG facilities. Imagery interpretation, if it is used exclusively for terrain analysis (such as identifying potential drug cultivation sites or drug producing laboratories, may be authorized.)

C-8. Do personnel receive initial and annual IO briefings? Are the briefings documented?

C-9. What is the reporting chain for "questionable activities"? Are unit members aware of it? Do they understand that they do not have to use the chain of command to report them?

C-10. Teach to ensure key personnel are familiar with requirements.

Glossary

Section I
Abbreviations

ACCO
Army Central Control Office

ADSW
Active Duty for Special Work

AF
Air Force

AFI
Air Force Instruction

AR
Army Regulation

ANG
Air National Guard

ANGI
Air National Guard Instruction

ARNG
Army National Guard

CD
Counterdrug

CI
Counterintelligence

CNGB
Chief, National Guard Bureau

DoD
Department of Defense

DOIM
Directorate of Information Management

EO 12333
Executive Order No. 12333

FOIA
Freedom of Information Act

IG
Inspector General

IO
Intelligence Oversight

IMINT
Imagery Intelligence

LEA
Law Enforcement Agency

MACOM
Major Army Command

METL
Mission Essential Task List

MOU
Memorandum of Understanding

NG
National Guard

NGB
National Guard Bureau

NGB-AIS
National Guard Bureau - Information Systems Directorate

NGB-IG
National Guard Bureau - Inspector General

NGB-IGI
National Guard Bureau - Inspector General Inspections

NGR
National Guard Regulation

NSA
National Security Agency

ODT
Overseas Deployment Training

OIP
Organizational Inspection Program

OPSEC
Operations Security

OSINT
Open-Source Intelligence

PAO
Public Affairs Officer

POTO
Plans, Operations, and Training Officer

SCIF
Sensitive Compartmented Information Facility

SIGINT
Signals Intelligence

SJA
Staff Judge Advocate

SSBI
Single Scope Background Investigation

STU III
Secure Voice / Data Terminal

SSO
Special Security Office

STARC
State Area Command

TAG
The Adjutant General

TS
Top Secret

U. S.
United States

USSIDs
United States Signals Intelligence Directives

Section II
Terms

Counterdrug Support Program
Support provided to federal, state or local LEAs and other civil authorities to assist with drug interdiction and other counterdrug support authorized in support of the National Drug Control Strategy.

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.

Intelligence Activities
Refers to all activities that DoD intelligence components are authorized to undertake pursuant to Executive Order 12333.

Intelligence Oversight Officer
The Officer, Warrant Officer or NCO (E7 or above) who have been appointed to administer the Intelligence Oversight Program (as an additional duty) in a unit. A primary and alternate IO monitor should be appointed on orders. At least one should be present whenever intelligence activities are conducted.

Law Enforcement Agency (LEA)
An organization, or a coordinating council comprised of several LEAs, empowered by local, state, or federal law to investigate, enforce or prosecute criminal laws regarding illegal drugs and controlled substances.

Questionable Activity
An undefined term referring to any intelligence activity which may violate the law, any Executive Order or Presidential directive, including EO 12333, or any applicable DoD policy.

Signals Intelligence
A category of intelligence including communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, either individually or in combination.

States
For the purpose of this regulation the term "states" includes all 50 states, the Commonwealth of Puerto Rico, the U.S. Virgin Islands, Guam and the District of Columbia.

United States Person
The term "United States person" means:

a. A United States citizen.

b. An alien known by the DoD intelligence component concerned to be a permanent resident alien.

c. An unincorporated association substantially composed of United States citizens or permanent resident aliens.

d. 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 United States person.

By Order of the Secretaries of the Army and the Air Force:

EDWARD D. BACA
Lieutenant General, USA
Chief, National Guard Bureau

Official:

DEBORAH GILMORE
Chief
Administative Services

Distribution: B/F