National Guard Regulation 20-10/Air
National Guard Instruction 14-101

Assistance, Inspections, Investigations and Follow-up

National Guard Inspector General Intelligence Oversight Procedures

National Guard Bureau
Arlington, VA 22202-3231
13 June 2011

UNCLASSIFIED

SUMMARY of CHANGE

NGR 20-10/ANGI 14-101
National Guard Intelligence Oversight Procedures
13 June 2011

This publication has been extensively revised.

National Guard Bureau ***NGR 20-10/ANGI 14-101**
Arlington, VA 22202-3231
13 June 2011

Assistance, Inspections, Investigations, and Follow-up

National Guard Inspector General Intelligence Oversight Procedures

By Order of the Secretary of Defense:

CRAIG R. MCKINLEY
General, USAF
Chief, National Guard Bureau

Official:
GARY SZABO
Col, USAF
Chief, Strategy and Policy Division

History. This publication supersedes NGR 20-10/ANGI 14-101, 15 Sep 95.

Summary. This regulation provides guidance for National Guard Inspectors General while implementing oversight of intelligence and intelligence related activities.

Applicability. This regulation addresses procedures that apply to all National Guard Inspectors General to assist in their execution of Intelligence Oversight (IO) responsibilities.

Proponent and exception authority. The proponent of this regulation is the National Guard Bureau - Inspector General (NGB-IG). The proponent has the authority to approve exceptions to this regulation that are consistent with controlling law and regulation. The proponent may delegate this authority in writing to the Chief, Intelligence Oversight Division, NGB-IG.

Management control process. This regulation is subject in part to the requirements of DOD Directive (DODD) 5240.01, AR 20-1 and AFI 90-201.

Supplementation. Supplementation of this regulation is prohibited without prior approval from Chief, National Guard Bureau, ATTN: NGB-IG, 1411 Jefferson Davis Highway, Suite 3100, Arlington, VA 22202-3231. State memorandums, pamphlets, standard operating procedures (SOPs), guides, regulations, etc. may not alter the policies established by this regulation.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Chief, National Guard Bureau, ATTN: NGB-IG, Suite 1D163 1636 Defense Pentagon Washington, DC 20301-1636.

Distribution. This publication is available in electronic media only and is intended for command levels A through E for the Army National Guard of the United States (ARNGUS), A through D for Active Army and United States Army Reserve (USAR) command levels with ARNGUS Soldiers assigned or attached or a command relationship with their units; and command level E for the Active Army and the USAR.

*This publication supersedes NGR 20-10/ANGI 14-101, 15 Sep 95.

Contents (Listed by paragraph number)

Chapter 1
Introduction

1-1. Purpose
This regulation prescribes the policies, procedures, responsibilities, and guidance for National Guard Inspectors General (IG) to assist in their execution of Intelligence Oversight (IO) responsibilities. IO involves a balancing of two fundamental interests: collecting information required to protect national security and protecting the individual rights of US persons (USPERS) as guaranteed by the Constitution and the laws of the United States (US). Although the primary focus of IO is to ensure that units and staff organizations conducting intelligence activities do not infringe on or violate the rights of USPERS, it is important to note that IO is applicable to all intelligence and intelligence related activities regardless of whether they are conducted by intelligence personnel or not. Commanders, Senior Intelligence Officers (SIOs), IGs, and judge advocates need to be cognizant of IO policies and requirements at all levels.

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

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

1-4. Responsibilities
a. The National Guard Bureau Office of the Inspector General Intelligence Oversight Division (NGB-IGO) will provide additional IG oversight of all intelligence, intelligence-related, Counterintelligence (CI), Defense Support to Civilian Authorities (DSCA), Domestic Operations (DOMOPS), and Counterdrug support program (CD) information gathering activities within the National Guard (NG). This includes the National Guard Bureau, the Office of the Chief, the Army and Air National Guard Directorates, and the 54 State and Territory Joint Force Headquarters. NGB-IGO specific functions include, but are not limited to:

(1) Serving as an NGB IO subject matter expert.

(2) Assisting State IGs execute their DODD 5240.01, AR 20-1 and AFI 90-201 IO functions.

(3) Conducting inspections of NG components that engage in intelligence and intelligence related activities, as directed by CNGB, ensuring compliance with law, Department of Defense (DoD), Departmental and NG requirements and regulations.

(4) Conducting investigations of questionable intelligence activities of NG components that engage in intelligence and intelligence related activities.

(5) Monitoring investigations and inspections by DoD components and other government agencies of NG components that engage in intelligence and intelligence related activities.

(6) Reviewing NGB Joint, Army and Air Directorate proponent IO policies and recommending improvements (as needed).

(7) Communicating with the Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO)), Secretary of the Army Inspector General, Intelligence Oversight Division (SAIG-IO), the Secretary of the Air Force Inspector General (SAF/IG), and with other agencies as required.

b. Each State Inspector General will:

(1) Inspect intelligence and non-intelligence units conducting intelligence functions and related activities within their States as directed by The Adjutant General (TAG). The commander's OIP will normally determine the frequency of intelligence oversight inspections within the command. However, IGs at all levels will ensure that they inspect their intelligence components a minimum of once every two years. (Reference AR 20-1, 6.13d)

(2) Identify intelligence components and personnel performing intelligence functions (generally numbered military intelligence units and intelligence J2/G2/A2/S2 offices) and verify compliance with appropriate directives. They may also include security personnel with additional intelligence duties. Some of these dual-responsibility personnel may not realize that they are subject to the provisions of this regulation, DODD 5240.01, AR 381-10 or AFI 14-104.

(3) Ascertain whether any unit, organization, staff, or office not specifically identified as an intelligence element that is being used for any intelligence or related purposes and, if so, ensure that its activities comply with DODD 5240.01, AR 381-10 or AFI 14-104. (Reference E.O. 12333, 1.12 e.)

(4) Review, in consultation with the Staff Judge Advocate (SJA) and Attorney General as appropriate, any planned and on-going NG information collection activities.

(5) Determine if intelligence components or other elements performing intelligence or related activities are involved in questionable activities (Source: DOD Regulation 5240.1-R, Procedure 15).

(6) 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.

(7) Report all "questionable activities" five working days after discovery through Intelligence and IG channels. (Refer to Chapter 3 of this regulation)

(8) Forward copies of IO related findings/inspection reports to The Inspector General (TIG), ATTN: NGB-IGO.

(9) Coordinate with the SJA for interpretation of federal and state law and applicable directives as they relate to intelligence activities. Unresolved questions should be forwarded to NGB-IGO for coordination, resolution, or additional legal review.

Chapter 2
General

2-1. Executive Order 12333 (as amended)

Executive Order 12333 (as amended) governs the conduct of intelligence activities for agencies within the Intelligence Community. It provides implementing instructions and establishes a balance between the rights of USPERS and the government's need for essential information. The order ensures:

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, as amended, procedures, agreed upon by the Attorney General and Secretary of Defense, have been promulgated by DoD Directive 5240.01 and DoD Regulation 5240.1-R. The Army has implemented the DoD directives through AR 381-10; the Air Force has implemented the DoD directives through AFI 14-104.

2-3. National Guard requirements

DoD Regulation 5240.1-R reestablishes the requirement for an Intelligence Oversight program in all NG intelligence and intelligence related activities. The procedures apply to the Office of the Chief, NGB, Army and Air NG intelligence units, activities, staffs, and personnel conducting intelligence activities directly related to a federal mission or duty in a Title 10 or Title 32 status. Additionally, the Service components guidance, AR 381-10 and AFI 14-104, further establish requirements for their respective NG elements.

2-4. Questionable intelligence activities

a. Military intelligence activities include all activities the defense intelligence components and non-intelligence organizations are authorized to undertake pursuant to stated references. A questionable intelligence activity is one that may violate law, Executive Orders or Presidential Directives, or applicable DoD regulations. One example of a questionable intelligence activity is the collection, retention, and dissemination of USPI without legitimate mission and authority. Questionable intelligence activities include but are not limited to:

(1) Gathering information about US domestic groups not connected with a foreign power or international terrorism

(2) Incorporating US Persons criminal information into an intelligence product

(3) Collecting USPI for force protection

(4) Collecting USPI from open sources without logical connection to unit mission or correlation to a validated collection requirement

(5) Indentifying a US Person by name in an Intelligence Information Report (IIR) without the requirement to do so

(6) Using one's status as an MI member to gain access for non-MI purposes

(7) Using MI counterintelligence (CI) badge and credentials (B&Cs) to represent oneself as an official beyond assigned MI responsibilities

(8) Using intelligence funds for personal gain; stealing a source's payments

(9) Falsifying intelligence reports

(10) Coaching a source or subject of an investigation prior to a polygraph in an effort to assist

b. NG organizations will report questionable intelligence activities through their chain of command to the State IG in accordance with Procedure 15, DOD 5240.1-R. IGs will forward such reports to NGB-IGO; NGB-IGO should receive such reports within 5 days of discovery. A questionable intelligence activity is one that may violate law, Executive Order, Presidential Directive, DOD Policy or Regulation, Service, Agency, or Command Policy or Regulation and is incident to an intelligence or an intelligence related activity. State IGs are encouraged to report what they perceive to be a questionable activity and seek assistance from NGB-IGO when appropriate.

c. State IGs will submit a quarterly report in standard memorandum format to NGB-IGO describing any actions taken relative to questionable intelligence activities previously reported, significant oversight activity, inspections or training accomplished during the quarter, along with any suggestions for improvement within five days after the close of each quarter. Negative reports, i.e. "Nothing Significant to Report" (NSTR) are required, unless otherwise directed. Requests for exception to these reporting requirements will be submitted to NGB-IGO.

Chapter 3
Guidance

3-1. Detailed Guidance

NG organizations that have an inherent intelligence function have an Intelligence Oversight Program. All established intelligence units have such a program. Newly formed units or activities will establish such a program. The Intelligence Oversight program will be included within AR 1-201, Organizational Inspection program (OIP) for the ARNG and AFI 90-201 (and subordinate command supplements) for the ANG. The IO program addresses 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 will know the identity of those responsible and will be aware of restrictions placed on their organization as well as the purpose of IO. Incoming personnel will receive oversight training within 30 days upon joining the unit and refresher training annually. Training will be included in the unit commander's Yearly Training Guidance.

b. NG military intelligence activities, units or staff organizations may collect USPI only when specifically authorized to do so by the Secretary of Defense in accordance with Executive Order 12333 (as amended), DoDD 5240.01, DoD Regulation 5240.1-R, AR 381-10, and AFI 14-104. USPI is defined as any information that can be used to identify a US citizen, permanent resident alien, unincorporated associations substantially composed of US citizens, or permanent resident aliens and corporations incorporated in the US and not directed or controlled by a foreign government. Information temporarily retained to determine whether mission and authority authorize retention cannot be held without positive determination for more than 90 days. NG military intelligence activities, units or staff organizations may analyze and share USPI that is lawfully resident in Intelligence Community (IC) databases, including DoD intelligence databases, for the purpose of giving NG commanders and staff situational awareness and indicators and warnings of foreign or transnational terrorist threats active in the US homeland. Collection and analysis of information, including USPI, that regards criminal activities and organizations having no foreign, transnational terrorist, or narcotics trafficking nexus will be handled strictly within Provost

Marshall (PM) and operational force protection channels. NGB and State JFHQ J2s, PMs, and J34 Staff Directorates provide NG leadership with information and recommendations on how to assist decision-making pertaining to Incident Awareness and Assessment (IAA), Force protection (FP), Anti-Terrorism (AT), Critical Infrastructure, Security and Law Enforcement (LE) activities.

c. State IGs will periodically test 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.

d. State IGs will verify that JFHQ staff members and program managers understand applicable DOD Regulation 5240-R procedures, Army National Guard unit commanders and program managers ensure that assigned personnel understand applicable AR 381-10 procedures and Air National Guard unit commanders and program managers ensure that assigned personnel understand applicable AFI 14-104.

e. The following types of units/programs have an IO program:

(1) State Joint Force Headquarter A2, G2 and J2 Sections

(2) Battalion, Brigade, Division S2/G2 staffs (ARNG)

(3) Military Intelligence Companies (ARNG)

(4) Military Intelligence Brigades/Battalions (ARNG)

(5) Special Forces Units/Special Operations Groups (ARNG)

(6) Information Operation Groups/Battalions (ARNG)

(7) Counterdrug Programs, coordinators, and staffs if they have requested military intelligence support (NGR 500-2/ANGI 10-801)

(8) Intelligence Squadrons and Reconnaissance Groups (ANG)

(9) Fighter, Interceptor and Airlift Unit Intelligence Staffs (ANG)

f. An IO Program should include but not limit to the following:

(1) Appoint an IO monitor in writing with appointment letter posted in work area

(2) Have on hand latest published versions of EO 12333, DODD 5240.01, DOD 5240.1-R, AR 381-10 or AFI 14-104 and NGR 20-10 (hard copy or digital versions are acceptable)

(3) Command directives

(4) Conduct and document initial orientation of new personnel within 120 days of arrival

(5) Conduct and document recurring training at least on an annual basis

(6) Procedures to report any questionable activity under the guidelines of the IO program

(7) Documented periodic file review to ensure maintenance in accordance with the IO program

3-2. NG Intelligence Equipment

NG intelligence equipment is equipment that has been purchased with Intelligence relating funding and may only be operated by NG intelligence personnel in a Title 10 or Title 32 status to conduct missions and training related to foreign governments, transnational terrorists, and narcotics traffickers, except that NG imagery capabilities may support IAA when validated through a Proper Use Memorandum (PUM). Specialized NG intelligence equipment and facilities may be provided for the use of federal agencies, including federal law enforcement authorities with appropriate approvals and procedures.

3-3. State Active Duty

State Active Duty **(**SAD) personnel are prohibited from using DoD intelligence resources and DoD equipment while in a SAD status. NG personnel in a SAD status are being paid by the state and not considered to be functioning in a DoD capacity; such SAD personnel are not, therefore, authorized to perform intelligence collection operations. States may utilize intelligence personnel for non-intelligence missions while on SAD.

3-4. Counterdrug Activities

a. NG Counterdrug (CD) Programs do not conduct intelligence activities of their own in counterdrug missions. NG CD programs support the linguist and criminal intelligence analysis activities of LEAs. Criminal information derived from support to LEAs will not be retained by the National Guard. CD

Coordinators will coordinate with LEAs to ensure support of intelligence LEA operations is conducted in accordance with DOD 5140.1-R and other applicable directives and in the support role intended by CD Support Program policy. Intelligence oversight training will be included in doctrinal training given to each member at initial entry and repeated annually for all personnel. Please refer to NGR 500-2/ANGI 10-801.

b. 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 2 years following the completion of CD support to the related LEA.

3-5. Civil Support Teams and other Non-Intelligence Units

a. NG Civil Support Teams (CST) and other CBRNE Consequence Management Response Units or Response Force Packages advise and facilitate suspected Weapons of Mass Destruction (WMD) attacks, advises civilian responders on appropriate actions through on-site testing and expert consultation, and facilitates the arrival of additional state and federal military forces. These units will comply with provisions outlined in DODD 5200.27 concerning the handling of information related non-DoD affiliated persons.

b. While conducting operations, a CST could incidentally or otherwise collect USPERS information. Upon completion of operations, all information or files must be redacted of all USPERS information before being used in After Action Reviews (AARs), Mission Termination Packets or other follow up reports.

c. All non-intelligence NG units and activities will comply with provisions outlined in DODD 5200.27 concerning the handling of information concerning non-DoD affiliated persons.

3-6. Public Affairs

a. Media and public interest in IO and intelligence related activities can be intense and immediate. Participants in any IO activity will coordinate with Public Affairs Officers (PAOs) 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 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 PAO.

Appendix A
References

Section I
Required Publications

AFI 14-104
Conduct of Intelligence Activities (Cited in paragraphs 1-4b (2), 1-4b (3), 2-2, 2-3, 3-1b, and 3-1 d, 3-1f (2))

AR 20-1
Inspector General Activities and Procedures (Cited in paragraph 1-4a (2))

AR 381-10
US Army Intelligence Activities (Cited in paragraphs 1-4b (2), 1-4b (3), 2-2, 2-3, 3-1b, 3-1d, 3-1f (2))

Constitution of the United States

DoDD 5240.01
DoD Intelligence Activities (Cited in paragraphs 1-4a (2), 1-4b (2), 1-4b (3), 2-2, 3-1b, 3-1f (2))

DoD 5240.1-R
Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons (Cited in paragraphs 1-4b (5), 2-2, 2-4b, 3-1b, 3-1f (2), 3-4)

DoDD 5200.27
Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense (Cited in paragraph 3-5a, 3-5c)

EO 12333, as Amended
United States Intelligence Activities (Cited in paragraphs 1-4b (3), 2-1, 3-1f (2))

EO 13462
President's Intelligence Advisory Board and Intelligence Oversight Board

The Privacy Act of 1974 Title 5, USC, Appendix 552a

Section II
Related Publications

AFI 90-201
Inspector General Activities

AR 525-13
Antiterrorism

AR 1-201
Organizational Inspection Program (OIP)

DoDD 5148.11
Assistant to the Secretary of Defense for Intelligence Oversight

Directive Type Memorandum 08-052
DoD Guidance for Reporting Questionable Intelligence Activities and Significant or Highly Sensitive Matters

NGR 500-2/ANGI 10-801
National Guard Counter Drug Support

Section III

Prescribed Forms
This section contains no entries.

Section IV

Referenced Forms
This section contains no entries.

Glossary

Section I
Abbreviations

ATSD (IO)
Assistant to the Secretary of Defense for Intelligence Oversight

CI
Counterintelligence

GEOINT
Geospatial Intelligence

HUMINT
Human Intelligence

IAA
Incident Awareness and Assessment

IC
Intelligence Community

IG
Inspector General

IMINT
Imagery Intelligence

INSCOM
Intelligence and Security Command

IP
Internet Protocol

LEA
Law Enforcement Agency

MASINT
Measurements and Signatures Intelligence

OSI
Office of Special Investigations, US Air Force

OSINT
Open Source Intelligence

PUM
Proper Use Memorandum

SAD
State Active Duty

SCI
Sensitive Compartmented Information

SIGINT
Signals Intelligence

SIO
Senior Intelligence Officer

TECHINT
Technical Intelligence

TIG
The Inspector General, Army

Section II

Terms

Administrative purposes
Information is collected for "administrative purposes" when it is necessary to administer the intelligence component, but is not collected directly in performance of an intelligence activity. Examples include general correspondence files; employment and disciplinary files; training records; in and out processing files; systems administration backup records; contractor performance records; personnel security clearance and access records; security manager duties; public affairs and legislative support materials. Administrative purposes may also include individual hand receipts and other logistics records staff actions, executive summaries and other information papers/briefings provided to senior leadership, and activity financial documents.

Collection
Information is collected when it is gathered or received by an employee in the course of official duties, and is intended for intelligence use. An employee must take an action that demonstrates intent to use or retain the information, such as producing an intelligence information or incident report or adding the information to an intelligence database. Data acquired by electronic means (for example, telemetry, signals traffic analysis, measurement and signatures intelligence) is "collected" only when it has been processed from digital electrons into a form intelligible to a human. Information that is held or forwarded to a supervisory authority solely for a collectability determination, and not otherwise disseminated within the intelligence component, is not "collected."

Concealed monitoring
Targeting a particular person or group without their consent, in a surreptitious and continuous manner, by electronic, optical, or mechanical devices. Monitoring is surreptitious when it is conducted in a manner designed to keep the subject unaware of it and continuous if conducted without interruption for a substantial time. Consensual intercept Electronic surveillance conducted after one or more, but fewer than all, of the parties to a communication consent to the interception.

Consent
An oral or written agreement by a person or organization to permit MI to take particular actions that affect the person or organization. Consent is implied upon adequate notice that a particular action carries the presumption of consent to an accompanying action (for example, notice that entering a building constitutes consent to being searched).

Counterintelligence (CI)
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. Jurisdiction for domestic CI activities lies with the Federal Bureau of Investigation (FBI). This delineation of responsibility is based on "The Agreement between the Deputy Secretary of Defense and Attorney General, dated April 5, 1979." A Secret (S) clearance is required to view this document. The Army Counterintelligence Coordinating Authority (ACICA) exercises technical control, review, coordination and oversight of Army CI controlled activities. It is the only Army organization which can authorize CI activities within the United States and territories. The Air Force Office of Special Investigations (AFOSI) provides professional investigative service to commanders of all Air Force activities. It is the primary organization responsible for AF counterintelligence services within the United States.

Delimitations agreement
Common term for the DOD/Department of Justice Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation.

Domestic activities
Activities within the United States that do not involve a significant connection with a foreign power, organization, or person.

Electronic surveillance
Electronic surveillance is composed of the following: the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known U.S. person who is in the United States, if the contents are acquired by intentionally targeting that U.S. person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes; the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, but does not include the acquisition of those communication of computer trespassers that would be permissible under Title 18 USC §2511(2)(i); the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes (see 50 USC §1801(f)).

Force protection
A commander's program to protect personnel, family members, facilities, and material, in all locations and situations. It is accomplished through the planned and integrated application of operations security, combating terrorism, physical security, base defense, personal protective services, law enforcement and crime prevention. The program is supported by intelligence, counterintelligence, and other security programs (see DODI 2000.16, AR 525–13 and AFI 31-210).

Foreign intelligence
Information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists.

Foreign power
Any foreign government, whether or not recognized by the United States, foreign-based political party or faction thereof, foreign military force, foreign-based terrorist group, or any organization composed, in major part, of any such entity or entities.

Geospatial Intelligence
GEOINT and Imagery Intelligence (IMINT) include full motion video (FMV), photographic, infrared, radar, and electro-optic images captured using ground or aerial based systems and other technical means.

Human Intelligence
HUMINT is a category of intelligence derived from information collected and provided by human sources. Typical HUMINT activities consist of interrogations and conversations with persons having access to pertinent information. The manner in which HUMINT operations are conducted is dictated by both official protocol and the nature of the source of the information. Within the context of the NG, HUMINT activity generally does not involve clandestine activities.

Incidental collection
Information about a non-targeted U.S. person received during an authorized intelligence activity.

Intelligence activities
Activities necessary for the conduct of foreign relations and the protection of the national security, including: collecting information needed by the President, the National Security Council, the Secretaries of State and Defense, and other Executive Branch officials for the performance of their duties and responsibilities; Intelligence dissemination and production; collecting information concerning, and conducting activities to protect against, intelligence activities directed against the United States, international terrorist and international narcotics activities, and other hostile activities directed against the United States by foreign powers, organizations, persons, and their agents; special activities; administrative and support activities within the United States and abroad necessary for performing authorized activities; such other intelligence activities as the President may direct from time to time (see EO 12333, as amended by EOs 13284,13355, and 13470). Intelligence activities are sometimes performed by non-intelligence individuals; intelligence oversight is applicable and not only limited to designated intelligence personnel.

Intelligence Community (IC)
(1) The Office of the Director of National Intelligence; (2) The Central Intelligence Agency; (3) The National Security Agency; (4) The Defense Intelligence Agency; (5) The National Geospatial-Intelligence Agency; (6) The National Reconnaissance Office; (7) The other offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs; (8) The intelligence and counterintelligence elements of the Army, the Navy, the Air Force, and the Marine Corps; (9) The intelligence elements of the Federal Bureau of Investigation; (10) The Office of National Security Intelligence of the Drug Enforcement Administration; (11) The Office of Intelligence and Counterintelligence of the Department of Energy; (12) The Bureau of Intelligence and Research of the Department of State; (13) The Office of Intelligence and Analysis of the Department of the Treasury; (14) The Office of Intelligence and Analysis of the Department of Homeland Security; (15) The intelligence and counterintelligence elements of the Coast Guard; and (16) Such other elements of any department or agency as may be designated by the President, or designated jointly by the Director and the head of the department or agency concerned, as an element of the Intelligence Community.

International terrorist activities
Activities undertaken by or in support of terrorist or terrorist organizations that occur totally outside the US, or that transcend national boundaries in the manner by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which the perpetrators operate or seek asylum.

Measurements and Signatures Intelligence
MASINT is technically derived information from either sensor sets or other means not classified as SIGINT, HUMINT or GEOINT/IMINT that results in intelligence that detects and classifies targets, and identifies or describes signatures (distinctive characteristics) of fixed or dynamic target sources. Images and signals from other intelligence-gathering processes can be further examined through the MASINT discipline—for example, to determine the depth of buried objects in imagery gathered through the IMINT process.

Open Source Intelligence
OSINT is intelligence collection that involves acquiring information from publicly available sources and analyzing it to produce actionable intelligence. In the intelligence community (IC), the term "open" refers to overt, publicly available sources. This includes, but is not limited to, media (such as newspapers, magazines, radio and television), computer-based information (such as internet-based communities, user generated content, social-networking sites, video sharing sites, and blogs) and official public data or other government reports (such as budgets, demographics, hearings, legislative debates, press conferences and public speeches).

Organization
Corporations and other commercial entities, academic institutions, clubs, professional societies, associations, and other groups whose existence is formalized in some manner or otherwise function on a continuing basis.

Organization within the United States
All organizations physically located within the United States' geographical boundaries, whether or not the organization is a US person.

Physical search
Physical search includes any intrusion upon a person or a person's property or possessions to obtain property or information. It does not include areas that are in plain view and visible to the unaided eye if no physical trespass occurs, abandoned property left in a public place, or any intrusion authorized as necessary to accomplish lawful electronic surveillance. Physical search includes also includes any physical intrusion within the United States into premises or property (including examination of the interior of property by technical means) that is intended to result in a seizure, reproduction, inspection, or alteration of information, material, or property, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes (see Title 50 USC §1821(5)).

Physical surveillance
Systematic and deliberate observation of a person by any means on a continuing basis. Acquiring a nonpublic communication by a person not party to it or not visibly present, through any means not involving electronic surveillance (that is, not intercepting and/or recording the communication).

Publicly available
The information has been published or broadcast in media available to anyone who wishes to obtain it. Examples include unrestricted web pages, books, newspapers, magazines, professional journals, radio, public address systems and television.

Questionable intelligence activity
Conduct during or related to an intelligence activity that may violate law, Executive Order or Presidential Directive, or applicable DOD or Army policy, including this regulation.

Retention
Refers to maintaining information about USPERS information that can be retrieved by the person's name or other personal identifying data.

Signals Intelligence
SIGINT is intelligence-gathering by interception of signals, whether between people or involving electronic signals not directly used in communication, or combinations of the two. As sensitive information is often encrypted, signals intelligence often involves the use of cryptanalysis. The National Security Agency (NSA) is the only organization which can authorize real-world Signals Intelligence collection activities. SIGINT is heavily regulated because it involves electronic surveillance, the most intrusive kind of search covered by the Fourth amendment to the US Constitution. Units involved in SIGINT will be aware of the US Signals Intelligence Directives (USSIDs) 18 (S), 1600NG (ARNG) (S) and 3500NG (ANG) (S). These

regulations dictate performance boundaries within SIGINT training and operations. These documents 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.

United States person
A United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien (a "green card" holder), an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

Section III

Special Abbreviations and Terms
This section contains no entries.