CHIEF NATIONAL GUARD BUREAU INSTRUCTION

NGB-IG
DISTRIBUTION: A

CNGBI 0700.01
09 June 2013

INSPECTOR GENERAL INTELLIGENCE OVERSIGHT

References: See Enclosure B.

1. Purpose. This instruction prescribes policies, responsibilities, and guidance for the National Guard Bureau Office of the Inspector General, Intelligence Oversight Division (NGB-IGO) to assist in its execution of Intelligence Oversight (IO) responsibilities consistent with references a, b, c and d. IO involves balancing two fundamental interests: collecting information required to protect national security and protecting the individual rights of U.S. persons (USPERs) as guaranteed by the U.S. Constitution and the laws of the U.S.

2. Cancellation. National Guard Regulation (NGR) 20-10/ Air National Guard Instruction (ANGI) 14-101 dated 13 June 2011 is hereby cancelled.

3. Applicability. This instruction is applicable to the NGB-IGO mission to assist in the execution of IO responsibilities and all intelligence and intelligence-related activities regardless of whether they are conducted by intelligence personnel or not. Commanders, Senior Intelligence Officers (SIO), Inspectors General (IG) and Judge Advocates (JA) need to be cognizant of IO policies and requirements at all levels.

4. Policy. NG organizations, units, and activities that have an inherent intelligence function, will have an IO Program. The NGB-IGO and State IGs will ensure that IO programs address and document, at minimum, areas outlined in Enclosure A.

5. Definitions. See Glossary.

6. Responsibilities.

a. NGB-IGO. NGB-IGO will provide additional IG oversight to all intelligence, intelligence-related, Counterintelligence (CI), Defense Support of

Civilian Authorities, Domestic Operations, and Counterdrug (CD) support program information gathering activities within the NG. This includes the Office of the Chief, National Guard Bureau (OCNGB), the Army and Air National Guard (ARNG/ ANG) directorates, the National Guard Joint Staff (NGJS) the 54 States, Territories and Joint Force Headquarters-State (JFHQ-State). Additional NGB-IGO responsibilities include, but are not limited to:

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

(2) Assisting State IGs in executing IO functions in accordance with (IAW) references a, b, c and d.

(3) Conducting inspections and ensuring compliance of NG components that engage in intelligence and intelligence-related activities, as directed by CNGB IAW law, Executive orders, Department of Defense (DoD) and other NG requirements and policy guidance.

(4) Conducting investigations of questionable intelligence activities (QIA) of NG components that engage in intelligence and intelligence-related activities as described in reference b.

(5) Monitoring investigations and inspections by the DoD, NG, and other government agency components that engage in intelligence and intelligence-related activities.

(6) Reviewing NGJS, ARNG, and ANG directorate proponent IO policies and recommending improvements.

(7) Communicating with the Assistant Secretary of Defense for Intelligence Oversight, the Secretary of the Army Inspector General, Intelligence Oversight Division, the Secretary of the Air Force Inspector General and other agencies as required.

b. State IG. State IGs will:

(1) Inspect all intelligence and non-intelligence units conducting any intelligence function and/or related activities within their States as directed by The Adjutant General (TAG). The commander's Organizational Inspection Program will normally determine the frequency of IO inspections within the command. However, IGs at all levels will ensure that they inspect their intelligence components at minimum of once every two years (see reference d).

(2) Identify intelligence components and personnel performing intelligence functions, generally numbered military intelligence units and National Guard (NG)-J2/G2/S2 (Army)/A2/IN (Air) intelligence offices regardless of unit size and verify compliance with appropriate directives.

Security personnel with additional intelligence duties and dual-responsibility personnel may be included and are subject to the provisions of this instruction and reference a.

(3) Ascertain whether any unit, organization, staff, or office, not specifically identified as an intelligence element, is being used for an intelligence or related purpose; and if so, ensure those activities comply with references a, e, and f IAW reference g.

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

(5) Determine if intelligence components or other elements performing intelligence or intelligence-related activities are involved in questionable activities (see reference b).

(6) Ensure procedures exist within organizations, staffs or offices used for intelligence purposes for the reporting of QIA.

(7) Report all QIA through Intelligence and IG channels to NGB-IGO.

(a) Report QIA of a serious nature and all significant or highly sensitive matters (see definition in glossary) immediately IAW reference e. Reports may be made by any secure means. Oral reports should be documented with a written report as soon as possible thereafter.

(b) Report QIA not of a serious nature (see definition in glossary) quarterly. Quarterly reports are due to the NGB-IGO by the 5th day of the month following the end of the quarter. Quarterly reports will describe all QIA as well as significant or highly sensitive matters identified during the quarter. Quarterly reports are required even if no reportable matters occurred during the reporting period.

(8) Forward copies of IO related findings/inspection reports to the NGB-IG office.

(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.

7. Summary of Changes. This is the initial publication of CNGBI 0700.01.

8. Releasability. This instruction is approved for public release; distribution is unlimited. NGB directorates, TAG, the Commanding General of the District of

Columbia, and JFHQ-State may obtain copies of this instruction through <http://www.ngbpdc.ngb.army.mil>.

9. Effective Date. This instruction is effective upon publication.

FRANK J. GRASS
General, USA
Chief, National Guard Bureau

Enclosures:
A -- Intelligence Oversight Program
B -- References
GL -- Glossary

ENCLOSURE A

INTELLIGENCE OVERSIGHT PROGRAM

1. A NG State/Unit/Section IO Program will address the following through documentation and practice.

a. IO Monitors. IO monitors are responsible for the IO program. They coordinate, conduct and record initial and annual refresher training. This training is included in the unit commander's Yearly Training Guidance. IO monitors fulfill all IO requirements IAW with references e and f. Quarterly reports are submitted through their chain of command to the State IG. Each organization assigns a primary and alternate IO monitor as an additional duty. IO monitors are identified and posted in the general work area. Unit personnel will know the identity of those responsible and must be aware of restrictions placed on their organization as well as the purpose of the IO. Incoming personnel receive initial oversight training within 90 days of joining the unit.

b. Lawful collection. NG military intelligence activities, units or staff organizations may collect United States Person Information (USPI) only when specifically authorized to do so by the Secretary of Defense IAW references a, e, f, and j. USPI is defined as any information that can be used to identify a U.S. citizen, permanent resident alien, unincorporated associations substantially composed of U.S. citizens or permanent resident aliens, or corporations incorporated in the U.S. 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, indicators, and warnings of foreign or transnational terrorist threats active on the U.S. homeland. Collection and analysis of information, including USPI, that regards criminal activities and organizations having no foreign, transnational terrorist, or narcotics trafficking connection are handled strictly within Provost Marshall (PM) and operational force protection channels. NGB and State JFHQ J2s, PMs, and NG-J34 (Anti-Terrorism/Force Protection (AT/FP)) staff directorates provide NG leadership with information and recommendations on how to assist decision-making pertaining to Incident Awareness and Assessment (IAA), and Critical Infrastructure and Law Enforcement Agencies (LEA).

c. State IGs will periodically test personnel within an intelligence organization to confirm whether they can identify regulations governing reporting procedures on QIA and the identity of the IO Officer.

d. State IGs will verify that JFHQ-State staff members and program managers understand applicable procedures IAW reference b. ARNG unit commanders and program managers will ensure assigned personnel understand applicable procedures IAW reference e. ANG unit commanders and program managers will ensure assigned personnel understand applicable procedures IAW reference f.

e. The following types of units/programs have an IO program: JFHQ-State A2(Air), G2(Army), and NG-J2 Sections; Battalion, Brigade, Division S2/G2 staffs (ARNG); Military Intelligence Companies/Battalions/ Brigades (ARNG); Special Forces Units/Special Operations Groups (ARNG); Information Operation Groups/Battalions (ARNG); units possessing unmanned aerial systems used for the purpose of collecting overhead imagery (ARNG); Intelligence Squadrons and Reconnaissance Groups (ANG); Fighter, Interceptor, Remotely Piloted Aircraft and Airlift Unit Intelligence Staffs (ANG). (Note: Homeland Response Force (HRF), Chemical, Biological, Radiological, and Nuclear and high yield Explosive Consequence Management Response (CBRNE) Enhanced Response Force Package (CERFP), and CD units along with Civil Support Teams (CST) must have USPER information programs (references c, j, k, and l, respectively.)

f. IO Program. The IO program will:

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

(2) Keep current copies of references a, e, f, g, and h.

(3) Conduct and document the initial orientation of new personnel within 90 days of arrival and recurring training annually.

(4) Conduct and document annual refresher training which must be conducted within a twelve month period.

(5) Maintain annual refresher training records for a period of five years.

(6) Detail procedures reported on any QIA.

(7) Document periodic file reviews to ensure maintenance IAW the IO program.

g. NG Intelligence Equipment. NG intelligence equipment is equipment purchased with intelligence-related funding and may only be operated by NG intelligence personnel in a Title 10 or Title 32 status in order to conduct

missions and training related to foreign governments, transnational terrorists and narcotics traffickers. This does not include NG imagery capabilities that may support Incident Awareness and Assessment (IAA) when validated through a Proper Use Memorandum. Specialized NG intelligence equipment and facilities may be used by federal agencies to include federal Law Enforcement Agency (LEA) authorities with appropriate approvals and procedures.

h. State Active Duty (SAD). SAD personnel are prohibited from using DoD intelligence resources and equipment while in a SAD status. NG personnel in a SAD status are paid by the state and are not considered as functioning in a DoD capacity. As a result, SAD personnel are not authorized to perform intelligence collection activities or operations. However, States may utilize intelligence personnel for non-intelligence missions while on SAD.

i. CD Activities.

(1) NG CD programs are governed by references j and k. NG CD programs support linguist and criminal intelligence analysis activities of LEAs and do not conduct intelligence activities during counterdrug missions. CD Coordinators will coordinate with LEAs to ensure support of intelligence LEA operations are conducted IAW reference j, k and other applicable directives, in a support role intended by CD Support Program policy. Criminal information derived from support to LEAs will not be retained by the NG. All such information is handled IAW reference j.

(2) Supported LEAs are responsible for obtaining legal authorization required to permit information gathering. A Memorandum of Understanding will be on file stating that this responsibility falls upon the supported LEA and will remain on file for a minimum of 2 years, per reference j, chapter 2, 2.9.

j. CST and other Non-Intelligence Units.

(1) NG CST, HRF, CERFP, and other CBRNE Units or Response Force Packages advise and facilitate consequence management of suspected Weapons of Mass Destruction attacks. They advise civilian responders on appropriate actions through on-site testing and expert consultation. Additionally, they facilitate the arrival of additional state and federal military forces. These units will comply with provisions outlined in references j and l concerning the handling of information related to non-DoD affiliated persons.

(2) While conducting operations, CSTs and/or other non intelligence entities could incidentally or otherwise collect information concerning persons or organizations not affiliated with the DoD. Upon completion of operations, all information, document records, and files must be redacted of all non DoD persons information before being used in After Action Reports, Mission

Termination Packets, or other follow-up reports, unless otherwise approved by the Secretary of Defense.

(3) IGs will ensure these units have a program in place that ensures compliance with law and regulation to include:

(a) Unit inspection checklists.

(b) Binders detailing the respective unit's IO program.

(c) Awareness training on handling information concerning persons or organizations not affiliated with the DoD.

k. Public Affairs.

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

(2) Personnel should refer media inquiries and other requests for information from outside of the NG/LEA channels to the PAO. The supported LEA shall lead the investigation concerning Public Affairs and make the final determination concerning the release of information in coordination with the PAO.

l. Information Operations. Information Operation units, sections, and or staffs will receive IO training yearly to de-conflict intelligence and information operations per para 5.7.4 of reference m.

m. Non-Intelligence NG Units/Personnel. All non-intelligence NG units and personnel will comply with provisions outlined in reference j concerning the handling of information concerning persons or organizations not affiliated with the DoD.

ENCLOSURE B

REFERENCES

a. DoD Directive 5240.01, 27 August 2007, “DoD Intelligence Activities"

b. DoD 5240.1-R, December 1982, “Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons”

c. AFI 90-201, 23 March 2012, “The Air Force Inspection System”

d. AR 20-1, 29 November 2010, “Inspector General Activities and Procedures”

e. AR 381-10, 03 May 2007, “U.S. Army Intelligence Activities”

f. AFI 14-104, 23 April 2012, “Conduct of Intelligence Activities”

g. Executive Order (E.O.) 12333, 04 Dec 1981 as amended 30 July 2008, “United States Intelligence Activities”

h. CNGB Instruction 2000.01, 17 September 2012, “National Guard Intelligence Activities”

i. CNGB Manual 2000.01, 26 November 2012, “National Guard Intelligence Activities”

j. DoD Directive 5200.27, 07 January 1980, “Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense”

k. NGR 500-2/ANGI 10-801, 29 August 2008, “National Guard Counter Drug Support”

l. NGR 500-3/ANGI 10-2503, 09 May 2011, “Weapons of Mass Destruction Civil Support Team Management”

m. DoD Directive 3600.01, 23 May 2011, “Information Operations (IO)”

n. 50 U.S.C. § 401A, “Definitions”

o. Field Manual 2.0, May 2004, “Intelligence”

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ANG	Air National Guard
ANGI	Air National Guard Instruction
ARNG	Army National Guard
CI	Counterintelligence
CD	Counterdrug
CBRNE	Chemical, Biological, Radiological, Nuclear and Explosive
CERFP	CBRNE Enhanced Response Force Package
CST	Civil Support Team
DoD	Department of Defense
GEOINT	Geospatial Intelligence
HRF	Homeland Response Force
HUMINT	Human Intelligence
IAA	Incident Awareness and Assessment
IAW	in accordance with
IG	Inspector General
IMINT	Imagery Intelligence
INSCOM	Intelligence and Security Command
IO	Intelligence Oversight
IP	Internet Protocol
LEA	Law Enforcement Agency
MASINT	Measurements and Signatures Intelligence
NGR	National Guard Regulation
OCNGB	Office of the Chief, National Guard Bureau
OSI	Office of Special Investigations, U.S. Air Force
OSINT	Open Source Intelligence
PAO	Public Affairs Officer
PM	Provost Marshall
QIA	questionable intelligence activities
SAD	State Active Duty
SJA	Staff Judge Advocate
SCI	Sensitive Compartmented Information
SIGINT	Signals Intelligence
SIO	Senior Intelligence Officer
USPER	United States Person
USPI	United States Person Information

PART II. DEFINITIONS

Administrative purposes -- Information collected for “administrative purposes” when 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, and public affairs and legislative support materials. Administrative purposes may also include individual hand receipts and other logistical records, staff actions, executive summaries, other information papers/briefings provided to senior leadership, and activity financial documents (see reference e).

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 action that demonstrates intent to use or retain the information, such as producing an intelligence information or incident report. 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” (see reference e).

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 (see reference e).

Consent -- An oral or written agreement by a person or organization to permit Military Intelligence 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) (see reference e).

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 (see reference e).

Delimitations agreement -- Common term for the DoD/Department of Justice agreement governing the conduct of DoD CI activities in conjunction with the Federal Bureau of Investigation (see reference e).

Domestic activities -- Activities within the U.S. that do not involve a significant connection with a foreign power, organization, or person (see reference e).

Electronic surveillance -- 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 USPER who is in the U.S. (see see reference e).

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 reference e).

Foreign intelligence -- Information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists (see reference m).

Foreign power -- Any foreign government, whether or not recognized by the U.S., 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 (see reference e).

Geospatial Intelligence (GEOINT) -- Includes full motion video, photographic, infrared, radar, and electro-optic images captured using ground or aerial based systems and other technical means (see reference n).

Human Intelligence (HUMINT) -- 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 (see reference n).

Incidental collection -- Information about a non-targeted USPER received during an authorized intelligence activity (see reference e).

Intelligence activities -- Activities necessary for the conduct of foreign relations and the protection of 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 U.S., international terrorist and international narcotics activities, and other hostile activities directed against the U.S. by foreign powers, organizations, persons, and their agents; special

activities; administrative and support activities within the U.S. and abroad necessary for performing authorized activities; such other intelligence activities as the President may direct from time to time (see reference e).

Intelligence Community (IC) -- A community comprised of the following organizations, listed in order of precedence: (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 (see reference m).

International terrorist activities -- Activities undertaken by or in support of terrorist or terrorist organizations that occur totally outside the U.S., 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 (see reference e).

Measurements and Signatures Intelligence (MASINT) -- 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 (see reference n).

Open Source Intelligence (OSINT) -- Intelligence collection that involves acquiring information from publicly available sources and analyzing it to produce actionable intelligence. In the intelligence community, 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) (see reference n).

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 (see reference e).

Organization within the U.S. -- All organizations physically located within the U.S. geographical boundaries, whether or not the organization is a USPER (see reference e).

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 searches also include any physical intrusion within the U.S. 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 reference e).

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) (see reference e).

Publicly available -- Information published or broadcasted in the media that is available for anyone. Examples include unrestricted web pages, books, newspapers, magazines, professional journals, radio, public address systems, and television (see reference e).

Questionable Intelligence Activity (QIA) – Per reference b, the term QIA refers to any conduct that constitutes, or is related to, an intelligence activity that may violate the law, any Executive order or Presidential directive, or applicable DoD, service or NGB policy. A QIA may be considered highly sensitive or significant in nature if the development or circumstance involving the intelligence activity or personnel could impugn the reputation or integrity of the DoD Intelligence Community or otherwise call into question the propriety of an intelligence activity. Such matters might be manifested in or by an activity:

(a) Involving congressional inquiries or investigations.

(b) That may result in adverse media coverage.

(c) That may impact on foreign relations or foreign partners.

(d) Related to the unauthorized disclosure of classified or protected information such as information identifying a sensitive source and method. Reporting under this paragraph does not include reporting of routine security violations (see reference g).

Retention -- Refers to maintaining information about USPERs information that can be retrieved by the person's name or other personal identifying data (see reference e).

Signals Intelligence (SIGINT) -- Intelligence-gathered 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 (see reference n).

The National Security Agency -- The only organization able to authorize real-world SIGINT activities (see reference n).

United States Person (USPER) -- A U.S. 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 U.S. citizens or permanent resident aliens; or a corporation incorporated in the U.S., except for a corporation directed and controlled by a foreign government or governments (see reference e).