



# CHIEF NATIONAL GUARD BUREAU INSTRUCTION

---

NGB-J2  
DISTRIBUTION: A

CNGBI 2000.01B  
04 April 2017

## NATIONAL GUARD INTELLIGENCE ACTIVITIES

References: See Enclosure B.

1. Purpose. This instruction establishes policy and assigns responsibilities for the conduct and oversight of National Guard (NG) intelligence and intelligence-related activities in accordance with (IAW) references a, b, and c.
2. Cancellation. This instruction cancels Chief of the National Guard Bureau (CNGB) Instruction 2000.01A, 24 July 2015, "National Guard Intelligence Activities" and CNGB Notice 2000, 12 October 2016, "Interim Revision to CNGB Series 2000.01, "National Guard Intelligence Activities."
3. Applicability. This instruction applies to all elements of the NG, to include Title 32 (T-32) NG Joint Force Headquarters-State (NG JFHQs-State), and T-32 NG intelligence units and staff organizations, and non-intelligence organizations that perform or train to perform intelligence or intelligence-related activities, hereinafter referred to as the NG intelligence component. In addition to references a and b, Army National Guard (ARNG) and Air National Guard (ANG) members serving in a Title 10 (T-10) status must comply with Service-specific guidance IAW references d and e, respectively.
4. Policy. It is National Guard Bureau (NGB) policy that NG intelligence personnel operating in a T-32 status, operate as members of the Department of Defense (DoD) intelligence component and must comply with all DoD guidance and Federal laws applicable to the component, to include all Intelligence Oversight (IO) rules IAW references a and b.
  - a. Federal intelligence and surveillance and reconnaissance (ISR) equipment will not be used for activities other than authorized Foreign Intelligence or Counterintelligence (CI) activities and their associated training unless approved by the Secretary of Defense (SecDef) or his or her designee

**UNCLASSIFIED**

IAW references a, b, and c.

b. NG intelligence personnel operating in a State active duty (SAD) status are not members of the DoD intelligence component and are prohibited from engaging in DoD intelligence and CI activities. NG personnel in SAD status are also prohibited from using DoD intelligence, ISR and CI equipment, such as the Joint Worldwide Intelligence Communications System, unless the SecDef or his or her designee authorizes that use IAW references a, b, and c.

c. NG personnel in SAD status are subject to the provisions of State law, including privacy laws. Certain information may be controlled by reference f. In most States, the collection, use, maintenance, and dissemination of U.S. person information (USPI) is strictly regulated; therefore, NG members in a SAD status should seek competent legal advice on applicable State laws before collecting information concerning USPI.

d. States may re-assign intelligence personnel to a non-intelligence mission while in SAD status, as long as they do not use or attempt to access intelligence, ISR, or CI systems, resources, or equipment, unless the SecDef or his or her designee authorizes that use IAW references a, b, and c.

e. NG intelligence organizations, units, and staff organizations, and non-intelligence organizations that perform intelligence or intelligence-related activities, such as Eagle Vision, cyberspace intelligence, and cyberspace ISR activities that could collect, analyze, process, retain, or disseminate information on U.S. persons, will establish IO programs IAW reference g.

f. NG information operation units, sections, and staffs will receive IO training annually to de-conflict intelligence and information operations IAW reference h.

g. All ARNG 18F series Military Occupational Specialty (MOS) soldiers and all other personnel trained and authorized to conduct Advanced Special Operations (ASO) IAW reference i are subject to IO policy IAW reference j. Soldiers who are 18F series MOS or ASO trained but are not attached or assigned to a section that conducts intelligence or intelligence-related activities are not subject to IO policy IAW reference j.

h. NGB-J2 will serve as the Defense Intelligence Component Head for the NG to carry out duties as assigned in reference a. When reference a permits delegation of authority for an action, authority is delegated to the G2 for the ARNG (ARNG-G2), to the A2 for the ANG (ANG-G2) and NG JFHQs-State J2s for the States, respectively.

04 April 2017

i. Senior Intelligence Officer (SIO) authority is delegated to the ARNG-G2 and ANG/A2/3/6/10 for management of ARNG and ANG Sensitive Compartmentalized Information (SCI) programs respectively.

j. Special Security Officer (SSO) appointments will be sent to the Defense Intelligence Agency and Under Secretary of Defense for Intelligence, and maintained locally.

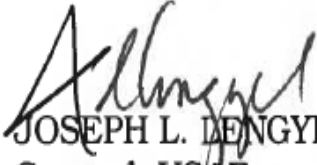
5. Definitions. See Glossary.

6. Responsibilities. See Enclosure A.

7. Summary of Changes. This instruction has been revised to incorporate changes to DoD IO policy contained in reference a. It designates NGB-J2 as the NG Defense Intelligence Component Head. It requires annual civil liberties and privacy protections training for all NG intelligence component personnel who access or use USPI. Furthermore, it requires documentation of the authority approving USPI retention. It adds rules for hosting shared repositories of data containing USPI. It also requires improper dissemination of USPI be treated and reported as a questionable intelligence activity (QIA).

8. Releasability. This instruction is approved for public release; distribution is unlimited. Copies are available through <<http://www.ngbpdc.ngb.army.mil>>.

9. Effective Date. This instruction is effective upon publication and must be reissued, cancelled, or certified as current within five years of its publication.



JOSEPH L. DENGYEL  
General, USAF  
Chief, National Guard Bureau

Enclosures:

- A -- Responsibilities
- B -- References
- GL -- Glossary

ENCLOSURE A

RESPONSIBILITIES

1. Director of the Joint Intelligence Directorate (NGB-J2). The Director of NGB-J2 will:

a. Oversee policy, unit budgeting, and staff management for NG joint intelligence activities.

b. Serve as the SIO for the NG, who is responsible for the protection and management of NG SCI programs in coordination with ANG and ARNG SIOs IAW references k, l, m, n, and o.

c. Liaise with the Intelligence Community on behalf of the CNGB on all matters concerning oversight of intelligence and intelligence-related activities.

d. Advise the CNGB and senior staff on all matters regarding the oversight of intelligence and intelligence-related activities, with particular emphasis on domestic applications.

e. Maintain situational awareness of the missions, plans, and capabilities of all NG intelligence and intelligence-related organizations, units, and staffs.

f. Review all joint proposals for intelligence activities and refer any that may be unlawful, or contrary to applicable Executive Branch or DoD derivative policies, to the Office of the NGB Chief Counsel (NGB-JA) for review.

g. Establish and maintain an IO program to ensure the legality and propriety of all NGB-J2 intelligence and intelligence-related activities.

h. Appoint, in writing, experienced intelligence professionals to serve as primary and alternate NGB-J2 IO Monitors; post copies of the appointment memorandum in the NGB-J2 workspaces, and maintain a file in the IO Continuity Binder.

i. Conduct required IO training for all personnel assigned or attached to NGB-J2, and maintain working knowledge of IO statutory and regulatory guidance, to include reporting responsibilities and all restrictions.

j. Ensure that all personnel assigned or attached to NGB-J2 who access or use USPI are trained annually on the civil liberties and privacy protections that apply to such information.

04 April 2017

k. Develop NGB-J2 procedures for retaining USPI, and for recording the reasons for retaining USPI and the authority for approving retention of USPI.

l. Conduct IO Staff Assistance Visits of NG JFHQs-State J2s, as required or requested.

m. Coordinate with NGB-JA and the office of the NGB Inspector General (IG) (NGB-IG) on IO matters, as required or requested.

n. Review and approve all T-32 Proper Use Memorandums (PUM) from NG JFHQs-State J2s in consultation with NGB-JA.

o. Review all NGB-J2 electronic and hard copy files at least once each calendar year IAW reference g to ensure that no unauthorized USPI has been retained. Retain a Memorandum for Record (MFR) on file in the IO Continuity Binder certifying the review.

p. Take reasonable steps to audit access to information systems containing USPI and periodically audit queries or other search terms to assess compliance with reference a.

q. Certify the proper use of all domestic commercial or publicly available imagery, such as U.S. Geological Survey (USGS) imagery, Google Earth imagery, and Falcon View imagery, through an internal MFR, and keep the certifications on file in the IO Continuity Binder IAW reference g.

r. Submit a quarterly IO Report to the NGB-IG IO Division (NGB-IGO) for all NGB (NGB-J2, ARNG-G2, and NGB/A2/3/6/10) activity IAW reference p.

s. Serve as the Chairperson and a voting member of the NGB IO Panel.

t. Be familiar with the requirement to report QIA, Significant/Highly Sensitive Matters (S/HSM), and certain Federal crimes and ensure that they are reported, and ensure that no retribution or adverse action is taken against any NGB-J2 personnel who reports these matters.

2. Director of C4 Systems and Chief Information Officer Directorate (CIO) (NGB-J6/CIO). The Director of NGB-J6/CIO will take reasonable steps to ensure effective auditing and reporting as required by reference a in developing and deploying information systems that are used for intelligence involving USPI.

3. NGB-IGO. NGB-IGO will:

- a. Comply with duties specified in reference p.
- b. Serve as a voting member of the NGB IO Panel.
- c. Receive initial and annual IO training and maintain a working knowledge of IO statutory and regulatory guidance, to include reporting responsibilities and all restrictions.

4. NGB-JA. NGB-JA will:

- a. Be familiar with the missions, plans, and capabilities of NGB-J2 and State intelligence and intelligence-related organizations and units, and all laws, Executive Orders (EO), policies, regulations, and instructions that apply to their activities, to include restrictions on the collection, retention, and dissemination of USPI, and QIA, S/HSM, and certain Federal crimes.
- b. Ensure that NGB-JA IO personnel receive IO training.
- c. Provide legal counsel for NGB-IO issues.
- d. Provide interpretations of applicable EOs, directives, regulations, and instructions, and also Federal, State, and tribal laws as they relate to intelligence and intelligence-related activities within NGB and NG JFHQs-State.
- e. Provide legal opinions and advice to NGB-J2 and NG JFHQs-State Judge Advocates (JA) on the legality and propriety of intelligence and intelligence-related activities.
- f. Review T-32 PUMs for legal sufficiency.
- g. Know the jurisdictional relationship between NG intelligence and CI activities, as well as the parallel jurisdictions of Antiterrorism/Force Protection (AT/FP) and law enforcement (LE) activities.
- h. Review NGB intelligence plans, proposals, and concepts for legality and propriety, as required.
- i. Assist in training NGB staff members engaged in intelligence and intelligence-related activities on all EOs, laws, policies, treaties, and agreements that apply to their activities.
- j. Serve as a voting member of the NGB IO Panel.

04 April 2017

5. DARNG. The DARNG will appoint the ARNG-G2 as the SIO for the ARNG to exercise staff responsibility for SCI and security programs, and overall readiness of the intelligence disciplines within the ARNG.
6. Director of ARNG-G2. The Director of ARNG-G2 will:
  - a. Oversee policy, unit budgeting, and staff management for ARNG intelligence activities.
  - b. Serve as SIO for the ARNG and exercise staff responsibility for SCI and security programs, and overall readiness of the intelligence disciplines within the ARNG: Geospatial Intelligence (GEOINT), to include Imagery Intelligence (IMINT), Signals Intelligence (SIGINT), HUMINT, CI, and All-Source Analysis.
  - c. Correspond with the Department of Army Deputy Chief of Staff for Intelligence (G2) regarding the oversight of ARNG intelligence activities.
  - d. Ensure that all personnel assigned or attached to ARNG-G2 receive required IO training, and know IO statutory and regulatory guidance, to include reporting responsibilities and all restrictions. ARNG units will be inspected by NGB-IG and may be inspected by the Senior DoD IO Official (SIOO) and gaining major command (MACOM).
  - e. Ensure that all personnel assigned or attached to ARNG-G2 who access or use USPI are trained annually on the civil liberties and privacy protections that apply to such information.
  - f. Develop ARNG-G2 procedures for retaining USPI, recording the reasons for retaining USPI and the authority for approving retention of USPI.
  - g. Submit ARNG-G2 data for a Quarterly IO Report to NGB-J2 IAW reference p. ARNG units will provide quarterly IO reporting to NGB-IGO through their NG JFHQs-State.
  - h. Serve as a voting member of the NGB IO Panel.
  - i. Take reasonable steps to audit access to information systems containing USPI and to periodically audit queries or other search terms to assess compliance with reference a.
7. Director of ARNG-G6. The Director of ARNG-G6 will take reasonable steps to ensure effective auditing and reporting as required by reference a when developing and deploying information systems that are used for intelligence involving USPI.

04 April 2017

8. DANG. The DANG will appoint the ANG/A2 as SIO for the ANG to exercise staff responsibility for SCI and security programs, and overall readiness of the intelligence disciplines within the ANG.

9. Director of ANG/A2/3/6/10. The Director of ANG/A2/3/6/10 will:

a. Oversee policy, unit budgeting, and staff management for ANG intelligence activities.

b. Serve as SIO for the ANG and exercise staff responsibility for SCI and security programs, and overall readiness of the intelligence disciplines within the ANG: GEOINT, to include IMINT, SIGINT, and All-Source Analysis.

c. Correspond with the Air Force (AF) Deputy Chief of Staff for Intelligence, Surveillance, and Reconnaissance regarding the oversight of ANG intelligence activities.

d. Ensure that all intelligence personnel assigned or attached to ANG/A2/3/6/10 receive required IO training, and know IO statutory and regulatory guidance, to include reporting responsibilities and all restrictions. ANG units will be inspected by NGB-IG and may be inspected by the DoD SIOO and gaining major command (MAJCOM).

e. Ensure that all intelligence component personnel assigned or attached to ANG/A2/3/6/10 who access or use USPI are trained annually on the civil liberties and privacy protections that apply to such information.

f. Develop ANG/A2/3/6/10 procedures for retaining USPI, recording the reasons for retaining USPI and the authority for approving retention of USPI.

g. Submit a Quarterly IO Report to NGB-J2 IAW reference p. ANG units will provide quarterly IO reporting to NGB-IG through their NG JFHQs-State and gaining MAJCOM.

h. Serve as a voting member of the NGB IO Panel.

i. Take reasonable steps to audit access to information systems containing USPI and to periodically audit queries or other search terms to assess compliance with reference a.

j. Take reasonable steps to ensure effective auditing and reporting as required by reference a in developing and deploying information systems that are used for intelligence involving USPI.



10. The Adjutants General (TAG) and the Commanding General of the District of Columbia National Guard (CG). TAGs and the CG will:

- a. Be knowledgeable of all State intelligence and intelligence-related activities.
- b. Appoint, in writing, an experienced professional to serve as the NG JFHQ-State J2.
- c. Develop and publish State IO policy and procedures that include:
  - (1) Internal procedures for determining if any USPI may be retained, recording the reasons for retaining USPI, and the authority for approving retention of USPI IAW reference a.
  - (2) Purging or redacting information that may not be retained.
  - (3) Marking all files containing USPI information IAW reference g.
  - (4) Conducting a yearly intelligence file review and certification to ensure that no unauthorized USPI has been retained.
- d. Receive initial and annual IO training.
- e. Be familiar with IO procedures, and assign tasks and missions IAW IO policy and guidance.

11. NG JFHQs-State J2. NG JFHQs-State J2s must possess a military intelligence MOS or AF Specialty Code and will:

- a. Be knowledgeable of all State intelligence and intelligence-related activities.
- b. Serve as the NG JFHQs-State SIO IAW references l, m, n and o.
- c. Appoint, in writing, a NG JFHQs-State SSO to manage NG JFHQs-State SCIF for TAG, IAW reference l.
- d. Establish and maintain an effective IO program for all personnel assigned or attached to NG JFHQs-State J2s.
- e. Appoint, in writing, experienced intelligence professionals to serve as NG JFHQs-State primary and alternate IO Monitors. Post copies of the appointments in the NGB-J2 workspaces and file them in the IO Continuity Binder.

- f. Conduct required IO training for all NG JFHQs-State intelligence component personnel, and know IO statutory and regulatory guidance, to include reporting responsibilities and all restrictions.
- g. Ensure all personnel assigned or attached to NG JFHQs-State J2 who access or use USPI are trained annually on the civil liberties and privacy protections that apply to such information.
- h. Identify intelligence staffs, units, and personnel performing intelligence and intelligence-related functions within the State, and verify compliance with appropriate directives. Dual-responsibility personnel are subject to the provisions of references q and r for non-intelligence duties.
- i. Advise TAG or the CG and his or her staff on matters related to the oversight of intelligence and intelligence-related activities and correspond with TAG or the CG regarding the State IO program.
- j. Coordinate with the State JA and IG on IO matters.
- k. Review, in consultation with the NG JFHQs-State IG, JA, and J3 any planned or on-going NG information-collection activities. Submit any required documentation.
- l. Submit, after consultation with the NG JFHQs-State JA, a PUM to NGB-J2 for any domestic imagery training, exercise, or real-world mission flown in a T-32 status IAW reference g.
- m. Review all NG JFHQs-State J2 electronic and hard copy files at least once each calendar year IAW reference g to ensure that no unauthorized USPI has been retained. Retain an MFR on file in the IO Continuity Binder certifying the review was accomplished.
- n. Certify the proper use of all domestic commercial or publicly available imagery, such as USGS imagery, Google Earth imagery, and Falcon View imagery, through an internal MFR IAW reference g at least once each calendar year and maintain on file in the IO Continuity Binder.
- o. Consolidate Quarterly IO Reports from all intelligence organizations, units and staff organizations, and non-intelligence organizations that perform intelligence or intelligence-related activities and submit a consolidated Quarterly IO Report to the NG JFHQs-State IG IAW reference o.

12. NG JFHQs-State IGs. NG JFHQs-State IG will:

- a. Comply with duties as specified in reference o.
- b. Receive initial and annual IO training and maintain a working knowledge of IO statutory and regulatory guidance, to include reporting responsibilities and all restrictions.

13. NG JFHQs-State JAs. NG JFHQs-State JAs will:

- a. Be knowledgeable of the missions, plans, and capabilities of State intelligence and intelligence-related entities, and the Federal and State laws, policies, and treaties that apply to their activities, to include the restrictions on collection, retention, and dissemination of USPI, and the requirement to report QIA, S/HSM and certain Federal crimes.
- b. Be knowledgeable of the jurisdictional relationship between NG intelligence and CI activities, as well as the parallel jurisdictions of AT/FP and Law Enforcement activities.
- c. Receive IO training IAW reference g.
- d. Advise TAG or the CG and NG JFHQs-State J2s on intelligence law and IO matters within their purview.
- e. Review intelligence plans, proposals, and concepts for legality and propriety.
- f. Review all State T-32 PUMs for legal sufficiency.
- g. Train members of organizations engaged in intelligence and intelligence-related activities on all laws, policies, treaties, and agreements that apply to their activities, as required.

14. Commanders, Directors, and SIOs. Commanders and Directors of intelligence or intelligence-related organizations, and SIOs will:

- a. Receive IO training IAW reference g.
- b. Be knowledgeable of the missions, plans, and capabilities of subordinate intelligence and intelligence-related units and levy tasks and missions IAW IO policy and guidance.
- c. Establish and maintain an effective IO program for all personnel assigned or attached to the organization. Command SIOs are responsible for

unit IO programs, such as a Division G2, a Brigade Combat Team, an Intelligence Officer, or a wing Intelligence (A2)/SIO.

d. Appoint, in writing, experienced intelligence professionals to serve as primary and alternate IO Monitors. Post copies of the appointments in the organization workspaces and file them in the IO Continuity Binder.

e. Conduct required IO training for all personnel assigned or attached to the organization, and know IO statutory and regulatory guidance, including the reporting responsibilities and all restrictions.

f. Ensure all personnel assigned or attached to the organization who access or use USPI are trained annually on the civil liberties and privacy protections that apply to such information.

g. Forward proposals for intelligence activities that may be questionable or contrary to policy to a Service JA and NG-JFHQs-State JA for review and submission to NGB-JA if required.

h. Protect all personnel who report QIA allegations from reprisal or retaliation. Report any threats of retaliation to the IG.

i. Impose appropriate sanctions upon any employees who violate the provisions of this instruction and other applicable policies.

j. Review all electronic and hard copy intelligence files at least once each calendar year IAW reference g to ensure that no unauthorized USPI has been retained. Retain an MFR on file in the IO Continuity Binder certifying the review has been accomplished.

k. Certify the proper use of all domestic commercial or publicly available imagery, such as USGS imagery, Google Earth imagery, and Falcon View imagery, through an internal MFR IAW reference g at least once a calendar year. Maintain the certifications in the IO Continuity Binder.

l. Submit a Quarterly IO Report to State IGs IAW reference p.

15. IO Monitors. IO Monitors will:

a. Receive IO Monitor Training IAW reference g.

b. Implement an IO program to educate and train intelligence personnel on applicable IO regulations and directives, as well as individual reporting responsibilities, and confirm personnel can identify, at a minimum, the purpose of the IO Program, the regulations and instructions governing IO, IO

rules impacting their mission, reporting procedures for QIA, S/HSM and Federal crimes, and the identity of the IO Monitors.

- c. Conduct IO training, and maintain records of this training for five calendar years, to include the dates personnel received training.
- d. Maintain an IO Continuity Binder IAW Enclosure N of reference g.
- e. Maintain copies of State IO policy and applicable references so they are available to the organization. References may be in hard copy or an electronic format.
- f. Perform a self-inspection in the final quarter of the calendar year, if the organization was not evaluated that year by an IG from one of the following organizations: the DoD Senior Intelligence Oversight Official, MACOM (Army) or MAJCOM (AF), or NGB.
- g. Assist in making determinations on collectability of USPI as detailed in Procedure 2 of reference g, and seek assistance from the unit, State JA, NGB-IG, or NGB-J2.
- h. Review all files, electronic and paper, at a minimum of once per calendar year to ensure that any USPI is retained IAW Procedure 4 of reference g and certify that all files have been reviewed through an MFR, which will be maintained on file in the IO Continuity Book.
- i. Immediately route QIA reports and reports of incidents or S/HSM as specified in Procedure 15 of reference g.
- j. Submit a quarterly IO report through the chain of command to the State IG. ANG units must provide a copy to their gaining MAJCOM.

16. Intelligence Component Personnel. All intelligence component personnel will:

- a. Understand the authorized mission of the organization to which they are assigned.
- b. Be familiar with Procedures 1-4, 12, 14, and 15 of references a, b and g, any other procedures applicable to the assigned unit's mission or discipline, this instruction, and any organization-specific regulation, instruction, or standard operating procedures concerning the intelligence mission or discipline.

c. Conduct intelligence activities IAW applicable law and policy, including references a, b, and g; this instruction; and the policy of the appropriate intelligence discipline, and not exceed the authorities granted by them.

d. Complete the organization's IO training within 90 days of the assignment/employment, as well as annual refresher training and re-deployment training.

e. Report any intelligence activity that may violate guiding laws or policies (QIA) as well as S/HSM and Federal crimes reported to the Attorney General of the U.S. IAW reference g.

f. Identify the organization's IO Monitor and know how to establish contact.

17. Other IGs. Other IGs responsible for organizations or units that perform intelligence or intelligence-related activities other than NG JFHQs-State IGs, such as an ARNG Division IG or ANG Wing IG, will:

a. Be knowledgeable of which intelligence, and non-intelligence units that perform intelligence and intelligence-related activities, come under IG jurisdiction, and understand the mission of each organization and which procedures in reference g apply.

b. Understand IG responsibilities as highlighted in Procedures 14 and 15 of reference g.

c. Ensure organizations performing intelligence functions have an established mechanism for reporting QIA, S/HSM and Federal crimes reported to the U.S. Attorney General.

d. Report QIA, S/HSM and Federal crimes reported to the U.S. Attorney General, and submit quarterly reports IAW references g and p.

e. Receive IO training IAW reference g.

18. State JA/Legal Advisors. State JAs/Legal Advisors responsible for organizations or units that perform intelligence or intelligence-related activities will:

a. Be knowledgeable of which intelligence, and non-intelligence units that perform intelligence or intelligence-related activities, come under JA jurisdiction, and understand the mission of each organization and which procedures in reference g and laws apply.

b. Understand JA responsibilities as highlighted in Procedures 14 and 15 of reference g.

- c. Review all unit intelligence plans, proposals, and concepts—including PUMs—for legality and propriety.
- d. Receive IO training IAW reference g.

ENCLOSURE B

REFERENCES

- a. DoD Manual 5240.01, 08 August 2016, "Procedures Governing the Conduct of Intelligence Activities"
- b. DoD 5240.1-R, Change 1, 08 August 2016, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons"
- c. Executive Order 12333, 04 December 1981, "United States Intelligence Activities," (as amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008))
- d. AR 381-10, 03 May 2007, "U.S. Army Intelligence Activities"
- e. AF Instruction 14-104, 05 November 2014, "Oversight of Intelligence Activities"
- f. Privacy Act, 5 U.S.C. § 552a (1974)
- g. CNGB Manual 2000.01, 26 November 2012, "National Guard Intelligence Activities"
- h. DoD Directive 3600.01, 02 May 2013, "Information Operations (IO)"
- i. USSOCOM Directive 525-5, 19 August 2004, "Advanced Special Operations" (S//NOFORN)
- j. Army Special Forces Policy Memo, 14 January 2008, "Intelligence Oversight Training Program"
- k. DoD Directive 5105.77, 30 October 2015, "National Guard Bureau (NGB)"
- l. DoD Manual 5200.01, Volume 1, 24 February 2012, "DoD Information Security Program: Overview, Classification and Declassification"
- m. DoD Manual 5105.21, Volume 2, 19 October 2012, "Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security"
- n. DoD Manual 5105.21, Volume 1, 19 October 2012, "Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security"
- o. DoD Manual 5200.01, Volume 3, 24 February 2012, DoD Information



Security Program: Protection of Classified Information

p. CNGB Instruction 0700.01, 09 June 2013, "Inspector General Intelligence Oversight"

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

r. CNGB Instruction 2400.00, 07 November 13, "Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense"

## GLOSSARY

### PART I. ACRONYMS

A2	Intelligence (Air Force)
AF	Air Force
ANG	Air National Guard
ARNG	Army National Guard
ASO	Advanced Special Operations
AT/FP	Anti-Terrorism/Force Protection
CG	Commanding General of the District of Columbia National Guard
CI	Counterintelligence
CNGB	Chief of the National Guard Bureau
DoD	Department of Defense
G2	Intelligence (Army)
GEOINT	Geospatial Intelligence
IAW	In accordance with
IG	Inspector General
IMINT	Imagery Intelligence
IO	Intelligence Oversight
ISR	Intelligence, Surveillance, and Reconnaissance
JA	Judge Advocate
MACOM	Major Command (Army)
MAJCOM	Major Command (Air Force)
MFR	Memorandum for Record
MOS	Military Occupational Specialty
NG	National Guard
NGB	National Guard Bureau
NGB-IG	Office of the National Guard Bureau Inspector General
NGB-JA	Office of the National Guard Bureau Chief Counsel
NGB-J2	Joint Intelligence Directorate
NG JFHQs-State	Joint Forces Headquarters-State
PUM	Proper Use Memorandum
QIA	Questionable Intelligence Activity
SAD	State Active Duty
SCI	Sensitive Compartmented Information
SecDef	Secretary of Defense
S/HSM	Significant/Highly Sensitive Matter
SIGINT	Signals Intelligence
SIO	Senior Intelligence Official
SSO	Special Security Officer
T-10	Title 10
T-32	Title 32
TAG	The Adjutants General

USGS  
USPI

United States Geological Survey  
United States Person Information

## PART II. DEFINITIONS

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

Crimes Reported to the Attorney General -- Any intelligence activity that has been or will be reported to the Attorney General, or that must be reported to the Attorney General as required by law or other directive, including crimes reported to the Attorney General as required by reference n.

Department of Defense Intelligence Components -- Department of Defense Intelligence Components include: the Defense Intelligence Agency; the National Geospatial-Intelligence Agency, the National Reconnaissance Office, the National Security Agency/Central Security Service, and the intelligence elements of the Active and Reserve components of the Military Departments, including the U.S. Coast Guard when operating as a service in the Navy.

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

Intelligence Activity -- All activities that Department of Defense Intelligence Components are authorized to undertake pursuant to reference b, and includes activities conducted by “non-intelligence” organizations.

Intelligence Oversight Monitor -- An individual assigned to establish and implement intelligence oversight procedures and training, to evaluate staff/unit personnel intelligence oversight knowledge, and resolve collectability determinations in consultation with his or her servicing Inspector General and legal advisor.

Intelligence-Related Activity -- Those activities outside the consolidated defense intelligence program that respond to operational commanders’ tasking for time-sensitive information on foreign entities; respond to national intelligence community tasking of systems whose primary mission is support to operating forces; train personnel for intelligence duties; provide an intelligence reserve; or are devoted to research and development of intelligence or related capabilities. Specifically excluded are programs that are so closely integrated with a weapon system that their primary function is to provide immediate-use targeting data.

National Guard Intelligence Component -- National Guard Bureau, Title 32 Joint Force Headquarters-State, and Title 32 National Guard intelligence units and staff organizations, and Title 32 non-intelligence organizations that perform intelligence or intelligence-related activities.

Questionable Intelligence Activity -- Any conduct that constitutes, or is related to, an intelligence activity that may violate the law, any executive order or Presidential directive, including references a and b, this instruction, and/or other National Guard Bureau, Army, and Air Force policy documents and instructions.

Senior Intelligence Official -- The highest ranking military or civilian official charged with direct foreign intelligence missions, functions, responsibilities within a department, agency, component, or element of an Intelligence Community organization.

Significant/Highly Sensitive Matter -- A development or circumstance involving an intelligence activity or intelligence personnel that could impugn the reputation or integrity of the Department of Defense Intelligence Community or otherwise call into question the propriety of an intelligence activity. Such matters might be manifested in or by an activity involving congressional inquiries or investigations; that may result in adverse media coverage; that may impact on foreign relations or foreign partners; or related to the unauthorized disclosure of classified or protected information, such as information identifying a sensitive source and method. This does not include reporting of routine security violations.

United States Person -- A United States citizen; an alien known by the Defense Intelligence Component concerned to be a permanent resident alien; an unincorporated association substantially composed of United States citizens or permanent resident aliens; and 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. A person or organization in the United States is presumed to be a United States person, unless specific information to the contrary is obtained. Conversely, a person or organization outside the United States, or whose location is not known to be in the United States, is presumed to be a non-United States person, unless specific information to the contrary is obtained.