CHIEF NATIONAL GUARD BUREAU INSTRUCTION

NGB-J2 CNGBI 2000.01C
DISTRIBUTION: A 14 August 2018

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 through d.

2. Cancellation. This instruction cancels and replaces Chief of the National Guard Bureau (CNGB) Instruction 2000.01B, 04 April 2017, "National Guard Intelligence Activities."

3. Applicability. This instruction applies to all elements of the NG.

4. Policy. It is NGB policy that NG intelligence personnel operating in a Title 32 (T32) 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, including all intelligence oversight (IO) rules IAW references b and c.

a. Federal intelligence and intelligence, surveillance, and reconnaissance (ISR) equipment as defined in the glossary is not used for activities other than authorized foreign intelligence or counterintelligence (CI) activities and associated training unless approved by the Secretary of Defense (SecDef) or his or her designee IAW references a through d.

b. In addition to references b, c, and d, Army National Guard (ARNG) and Air National Guard (ANG) members serving in a Title 10 status must comply with Service-specific guidance IAW references e and f, respectively.

c. In addition to references b, c, and d, T32 Guardsmen carrying out approved intelligence activity, such as Federated Intelligence Program or counterdrug Federal intelligence support, under the authorities of a combatant

command (CCMD), agency, or Service, must comply with the IO policy of the supported CCMD, agency, or Service (for example, Guardsmen conducting approved counterdrug intelligence activities in support of the National Security Agency [NSA] will comply with NSA intelligence oversight policy).

d. 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 and ISR equipment, such as the Joint Worldwide Intelligence Communications System or national or DoD CI and human intelligence (HUMINT) tools, such as the Counterintelligence/ Human Intelligence Automated Tool Set (CHATS) or Counterintelligence/ Human Intelligence Information Management System (CHIMS), or resources intended for CI and HUMINT activities, unless the SecDef or his or her designee authorizes that use IAW references a through d.

e. NG personnel in SAD status are subject to the provisions of State and Federal law, including privacy laws. Certain information may be controlled by reference g. In most States, the collection, use, maintenance, and dissemination of United States person information (USPI) is strictly regulated; therefore, unless command guidance is available, NG members in a SAD status should, through their chain of command, seek competent legal advice on applicable State laws before collecting information concerning United States persons.

f. States may reassign intelligence personnel to a non-intelligence mission while in a SAD status, as long as they do not use or attempt to access intelligence or ISR systems, resources, or equipment or CI national or DoD CI or HUMINT tools unless the SecDef or his or her designee authorizes that use IAW references a through d.

g. 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 USPI) will establish IO programs IAW reference h.

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

i. All ARNG 18F-series Military Occupational Specialty (MOS) Soldiers and all other personnel trained and authorized to conduct Advanced Special Operations (ASO) IAW reference j are subject to IO policy IAW reference k. 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 k.

j. Senior Intelligence Official (SIO) authority is delegated to the Director of ARNG Intelligence and Security Programs (ARNG-G2) and ANG Operations Directorate (ANG/A2/3/6/10) for management of ARNG and ANG Sensitive Compartmented Information (SCI) programs, respectively.

k. Special Security Officer 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 b. It requires appointment of an NGB IO Official (IOO) and defines the NGB IOO's responsibilities. It adds responsibilities for the NGB Directorate of Acquisitions (NGB-AQ) for contracts supporting the Joint Intelligence Directorate (NGB-J2). It also updates the Office of the Inspector General (NGB-IG) Intelligence Oversight Division (NGB-IGO) responsibilities.

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. LENGYEL
General, USAF
Chief, National Guard Bureau

Enclosures:

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

ENCLOSURE A

RESPONSIBILITIES

1. Director of NGB-J2. The Director of NGB-J2 will:

a. Serve as the Defense Intelligence Component head to carry out NG duties as assigned in references b and c. When references b or c permit delegation of authority for an action, authority is delegated to the Director of the ARNG-G2, ANG/A2/3/6/10, or NG Joint Force Headquarters–State (NG JFHQs-State) J2 for the States.

b. Oversee formation of policy, unit budgeting, and staff management for NG joint intelligence activities and development of IO implementing guidance.

c. Serve as the SIO for the NG, responsible for protection and management of NG SCI programs in coordination with ANG and ARNG SIOs IAW references l through o.

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

e. 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.

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

g. Appoint an NGB IOO who is of appropriate grade, has intelligence experience commensurate with his or her oversight responsibilities, has access to all component intelligence activities (including those protected by special access programs, alternative compensatory control measures, and other security compartments), and has direct access to the CNGB to report on NG IO compliance.

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 copies on file in the IO Continuity Binder.

i. Ensure that all personnel assigned or attached to NGB-J2, any other NGB personnel who conduct intelligence or intelligence-related activity, and NGB judge advocates (JAs) and inspectors general (IGs) who have IO responsibilities receive required IO training and maintain working knowledge of

IO statutory and regulatory guidance, including reporting responsibilities and all restrictions.

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

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. Review and approve all T32 Proper Use Memorandums (PUMs) from NG JFHQs-State J2s in consultation with NGB-JA.

m. Review all NGB-J2 electronic and hardcopy files at least once each calendar year IAW reference h to ensure that no unauthorized USPI has been retained and retain a Memorandum for Record (MFR) on file in the IO Continuity Binder certifying that the review was accomplished.

n. 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 c.

o. 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 h.

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

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

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

s. Provide the NGB-JA, NGB IG, DoD General Counsel, DoD SIOO, and any IG of competent jurisdiction with access to any employee and with all information necessary to perform their oversight responsibilities, including information protected by special-access programs, alternative compensatory control measures, or other security compartmentalization.

t. Ensure that Procurement Requirements Packages include the appropriate IO training and reporting of any QIA, S/HSM, or Federal crime IAW procedures defined in reference h.

2. NGB IO Panel. The NGB IO Panel will meet quarterly to discuss the legality and propriety of NG intelligence and intelligence-related activities, review NGB IO policy to ensure it is consistent with U.S. and DoD guidance, and analyze trends for quarterly reporting to the DoD Senior Intelligence Oversight Official (SIOO).

3. NGB IOO. The NGB IOO will:

a. Assist the CNGB and NGB-J2 in administering NGB and T32 NG IO.

b. Liaise with the Intelligence Community on behalf of the CNGB and NGB-J2 on all matters concerning oversight of intelligence and intelligence-related activities.

c. Advise the CNGB, NGB-J2, and other senior staff on all matters regarding the oversight of intelligence and intelligence-related activities, with particular emphasis on domestic applications.

d. Administer an IO training program tailored to mission requirements and provide initial and annual refresher IO training, including familiarity with the authorities and restrictions established in references a through d and other applicable intelligence policy, to all applicable employees.

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

f. Conduct periodic comprehensive reviews of all NGB and T32 NG intelligence and intelligence-related activities to verify compliance with Federal law, Executive Orders (EOs), Presidential directives, Intelligence Community Directives, and DoD Issuances and report significant findings to the DoD SIOO.

g. Periodically review component-produced intelligence products for compliance with applicable standards.

h. Coordinate with NGB-JA and NGB-IG on IO matters, as required or requested.

4. Director of Command, Control, Communications, and Computer Systems and Chief Information Officer (NGB-J6). The Director of NGB-J6 will take reasonable steps to ensure effective auditing and reporting as required by reference c in developing and deploying information systems that are used for intelligence involving USPI.

5. NGB-AQ. NGB-AQ will incorporate the customer-provided IO training and reporting of QIA, S/HSM, and Federal crimes IAW procedures established in the procurement requirements package and resulting contract actions.

6. NGB-IGO. NGB-IGO will:

a. Perform IO inspection and reporting responsibilities IAW references b and 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, including reporting responsibilities and all restrictions.

d. Comply with other duties specified in reference p.

7. NGB-JA. NGB-JAs 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, EOs, policies, regulations, and instructions that apply to their activities, including restrictions on the collection, retention, and dissemination of USPI and information on QIA, S/HSM, and 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 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 JAs on the legality and propriety of intelligence and intelligence-related activities.

f. Review T32 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 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.

k. Ensure that Procurement Requirements Packages include the appropriate IO training and reporting of any QIA or S/HSM IAW procedures defined in reference h.

8. Director of the ARNG. The Director of the ARNG will appoint the ARNG-G2 as the SIO to exercise staff responsibility for SCI and security programs and for overall readiness of the intelligence disciplines within the ARNG.

9. Director of ARNG-G2. The Director of ARNG-G2 will:

a. Oversee formation of 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, as well as overall readiness of the intelligence disciplines within the ARNG: geospatial intelligence (GEOINT), including imagery intelligence (IMINT), signals intelligence (SIGINT), HUMINT, CI, and all-source analysis.

c. Correspond with the Department of the Army G2 regarding the oversight of ARNG intelligence activities.

d. Ensure that all personnel within the ARNG staff who require IO training are trained and know IO statutory and regulatory guidance, including reporting responsibilities and all restrictions.

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 o. 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 c.

j. Ensure that Procurement Requirements Packages include the appropriate IO training and reporting of any QIA or S/HSM IAW procedures defined in reference h.

10. Director of the ARNG Chief Information Office (ARNG-G6). The Director of ARNG-G6 will take reasonable steps to ensure effective auditing and reporting as required by reference b when developing and deploying information systems used for intelligence involving USPI.

11. Director of the ANG. The Director of the ANG will appoint the ANG/A2/3/6/10 as SIO for the ANG to exercise staff responsibility for SCI and security programs and for overall readiness of the intelligence disciplines within the ANG.

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

a. Oversee formation of 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, including IMINT, SIGINT, and all-source analysis.

c. Correspond with the Air Force Deputy Chief of Staff for ISR regarding the oversight of ANG intelligence activities.

d. Ensure that all personnel within the ANG staff who require IO training are trained and know IO statutory and regulatory guidance, including reporting responsibilities and all restrictions.

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 major command.

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 c.

j. In developing and deploying information systems used for intelligence involving USPI, take reasonable steps to ensure effective auditing and reporting as required by reference c.

k. Ensure that Procurement Requirements Packages include the appropriate IO training and reporting of any QIA, S/HSM, or Federal crime IAW procedures defined in reference h.

13. The Adjutants General (TAGs) and the Commanding General of the District of Columbia (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 JFHQs-State J2.

c. Develop and publish State IO policy and procedures that include:

(1) Identifying all NG JFHQs-State, ARNG, and ANG staffs, organizations, and units in the State to which IO policy applies and which must maintain IO programs (for example, NG JFHQs-State J2; NG JFHQs-State IG and JA personnel responsible for intelligence staffs, units, or organizations; and any ARNG and ANG intelligence staffs, units, or organizations conducting intelligence or intelligence-related activity).

(2) State-specific training guidance.

(3) State QIA, S/HSM, and Federal crime reporting procedures.

(4) Self-inspection guidance.

(5) Procedures for filing PUMs and an annual MFR certifying proper use of domestic commercial or publicly available imagery.

(6) State procedures for requesting approval to use intelligence capabilities and assets (for example, procedures for requesting SecDef approval to use an MQ-9 drone for incident awareness and assessment).

(7) Internal procedures for determining whether any USPI may be retained, recording the reasons for retaining USPI and the authority for approving retention of USPI IAW reference h.

(8) Internal procedures for purging or redacting information that may not be retained.

(9) Internal procedures for marking all files containing USPI IAW reference h.

(10) Internal procedures for 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.

14. NG JFHQs-State J2. NG JFHQs-State J2s must possess a military intelligence MOS or Air Force 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 m through o.

c. Appoint, in writing, an NG JFHQs-State Special Security Officer to manage the NG JFHQs-State SCI Facility for TAG, IAW reference m.

d. Ensure that an effective IO program for all personnel assigned or attached to NG JFHQs-State J2s is established and maintained.

e. Appoint, in writing, experienced intelligence professionals to serve as NG JFHQs-State primary and alternate IO Monitors and post copies of the appointments in the NG JFHQs-State J2 workspaces and file them in the IO Continuity Binder.

f. Ensure that required IO training is given to all NG JFHQs-State intelligence component personnel and JA and IG personnel with IO responsibilities, and be familiar with IO statutory and regulatory guidance, including reporting responsibilities and all restrictions.

g. Ensure that all personnel assigned or attached to the 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 ongoing NG information-collection activities. Submit any required documentation.

l. After consultation with the NG JFHQs-State JA, submit a PUM to NGB-J2 for any domestic imagery training, exercise, or real-world mission flown in a T32 status IAW reference h.

m. Ensure that all NG JFHQs-State J2 electronic and hardcopy files are reviewed at least once each calendar year IAW reference g to ensure that no unauthorized USPI has been retained. Ensure that an MFR is maintained on file in the IO Continuity Binder certifying that 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 h at least once each calendar year and maintain the MFR 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 p.

p. Ensure that Procurement Requirements Packages include the appropriate IO training and reporting of any QIA, S/HSM, or Federal crime IAW procedures defined in reference h.

15. NG JFHQs-State IGs. The NG JFHQs-State IGs will:

a. Perform IO inspections and reporting responsibilities IAW references b and p.

b. Receive initial and annual IO training and maintain a working knowledge of IO statutory and regulatory guidance, including reporting responsibilities and all restrictions.

16. NG JFHQs-State JA. 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, including the restrictions on collection, retention, and dissemination of USPI and the requirement to report QIA, S/HSM, and 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 h.

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 T32 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.

17. Commanders, Directors, and SIOs of Intelligence or Intelligence-related Organizations. Commanders, Directors, and SIOs of intelligence or intelligence-related organizations, as well as other commanders and directors with intelligence or intelligence-related capabilities, will:

a. Receive IO training IAW reference h.

b. Be knowledgeable of the missions, plans, and capabilities of assigned and subordinate intelligence and intelligence-related capabilities and levy tasks and missions IAW IO policy and guidance.

c. Establish and maintain an effective IO program for all required personnel assigned or attached to the organization.

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 the copies in the IO Continuity Binder.

e. Ensure that all required personnel assigned or attached to the organization receive IO training and are familiar with IO statutory and regulatory guidance, including the reporting responsibilities and all restrictions.

f. Ensure that 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 NGB-IG.

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

j. Ensure that all electronic and hardcopy intelligence files are reviewed at least once each calendar year IAW reference g to ensure that no unauthorized USPI has been retained. Ensure that an MFR is maintained on file in the IO Continuity Binder certifying that 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 and maintain the certifications in the IO Continuity Binder.

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

18. IO Monitors. IO Monitors will:

a. Receive IO Monitor Training IAW reference h.

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 that 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 for all personnel within the staff, unit, or organization who require it, including intelligence personnel, other personnel conducting intelligence or intelligence-related activity, JAs, and IGs, and maintain records of this training for five calendar years, including the dates personnel received training.

d. Maintain an IO Continuity Binder IAW Enclosure N of reference h.

e. Maintain copies of State IO policy and applicable references so they are available to the organization. References may be in hardcopy or 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 the DoD SIOO, major command, or NGB.

g. Assist in making determinations on collectability of USPI as detailed in Procedure 2 of reference h and seek assistance from the unit, State JA, NGB-IG, or NGB-J2.

h. Review all files, electronic and paper, at least once per calendar year to ensure that any USPI is retained IAW Procedure 4 of reference h 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 h.

j. Submit a quarterly IO report through the chain of command to the State IG. ANG units must provide a copy to their gaining major command.

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

a. Understand the authorized mission and authorities of the organization to which they are assigned.

b. Be familiar with the policies contained in this instruction and Procedures 1-4 and 12, standards for employee conduct, and procedures for reporting QIA, S/HSM and federal crimes of references b, c, d, and h, any other procedures applicable to the assigned unit's mission or discipline and for employee conduct and identifying and reporting QIA, S/HSM, and Federal crimes listed in references b, c, d, and h, 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 b, c, d, and h; 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 or employment, as well as annual refresher training and re-deployment training.

e. Report any intelligence activity that may violate guiding laws or policies on QIA as well as S/HSM and Federal crimes reported to the United States Attorney General immediately upon discovery IAW reference h.

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

20. 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. Perform IO inspection and reporting responsibilities IAW references b and p.

b. Receive IO training IAW reference h.

21. State JAs and Legal Advisors. State JAs and 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 State JA jurisdiction and understand the mission of each organization and which procedures in reference g and laws apply.

b. Understand State JA responsibilities as highlighted in reference h.

c. Review all unit intelligence plans, proposals, and concepts, including PUMs, for legality and propriety.

d. Receive IO training IAW reference h.

ENCLOSURE B

REFERENCES

a. EO 12333, 04 December 1981, "United States Intelligence Activities," as amended by EOs 13284, 23 January 2003, "Amendment of Executive Orders, and Other Actions, in Connection With the Establishment of the Department of Homeland Security"; 13355, 27 August 2004, "Strengthened Management of the Intelligence Community"; and 13470, 30 July 2008, "Further Amendments to Executive Order 12333, United States Intelligence Activities"

b. DoD Directive 5148.13, 26 April 2017, "Intelligence Oversight"

c. DoD Manual 5240.01, 08 August 2016, "Procedures Governing the Conduct of DoD Intelligence Activities"

d. DoD 5240.1-R, December 1982, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons," Incorporating Change 2, 26 April 2017

e. Army Regulation 381-10, 03 May 2007, "U.S. Army Intelligence Activities"

f. Air Force Instruction 14-104, 05 November 2014, "Oversight of Intelligence Activities"

g. 5 United States Code, Section 552a (1974), "Privacy Act"

h. CNGB Manual 2000.01, 26 November 2012, "National Guard Intelligence Activities"

i. DoD Directive 3600.01, 02 May 2013, "Information Operations (IO)," Incorporating Change 1, 04 May 2017

j. United States Special Operations Command Directive 525-5, 19 August 2004, "Advanced Special Operations" (S//NOFORN)

k. Army Special Forces Policy Memo, 14 January 2008, "Intelligence Oversight Training Program"

l. DoD Directive 5105.77, 30 October 2015, "National Guard Bureau (NGB)," Incorporating Change 1, 10 October 2017

m. DoD Manual 5200.01, Volume 1, 24 February 2012, "DoD Information Security Program: Overview, Classification, and Declassification," Incorporating Change 1, 04 May 2018

n. DoD Manual 5105.21, Volume 1, 19 October 2012, "Sensitive

Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security," Incorporating Change 1, 16 May 2018, and Volume 2, 19 October 2012, "Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security," Incorporating Change 1, 05 April 2018

o. DoD Manual 5200.01, Volume 3, 24 February 2012, "DoD Information Security Program: Protection of Classified Information," Incorporating Change 2, 19 March 2013

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

GLOSSARY

PART I. ACRONYMS

A2	Intelligence (Air Force)
ANG	Air National Guard
ANG/A2/3/6/10	Air National Guard Operations Directorate
ARNG-G2	Army National Guard Deputy Chief of Staff for Intelligence and Security Programs
ARNG-G6	Director of the Army National Guard Chief Information Office
ASO	Advanced Special Operations
AT/FP	Antiterrorism and force protection
CCMD	Combatant command
CG	Commanding General of the District of Columbia
CHATS	Counterintelligence/Human Intelligence Automated Tool Set
CHIMS	Counterintelligence/Human Intelligence Information Management System
CI	Counterintelligence
CNGB	Chief of the National Guard Bureau
DoD	Department of Defense
EO	Executive Order
G2	Intelligence (Army)
GEOINT	Geospatial intelligence
HUMINT	Human intelligence
IMINT	Imagery intelligence
IAW	In accordance with
IG	Inspector general
IO	Intelligence oversight
IOO	Intelligence Oversight Official
ISR	Intelligence, surveillance, and reconnaissance
J3	Domestic Operations Directorate
JA	Judge advocate
MFR	Memorandum for Record
MOS	Military Occupational Specialty
NG	National Guard
NGB	National Guard Bureau
NGB-AQ	Directorate of Acquisitions
NGB-IG	Office of the Inspector General
NGB-IGO	Inspector General Intelligence Oversight Division
NGB-JA	Office of the Chief Counsel
NGB-J2	Joint Intelligence Directorate
NGB-J6	Command, Control, Communications, and Computer Systems and Chief Information Officer

NG JFHQs-State	National Guard Joint Force Headquarters–State
NSA	National Security Agency
PUM	Proper Use Memorandum
QIA	Questionable intelligence activity
SAD	State active duty
SCI	Sensitive Compartmented Information
SecDef	Secretary of Defense
S/HSM	Significant or Highly Sensitive Matters
SIGINT	Signals Intelligence
SIO	Senior Intelligence Official
SIOO	Senior Intelligence Oversight Official
T32	Title 32
TAG	The Adjutant General
USGS	United States Geological Survey
USPI	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 a.

Department of Defense Intelligence Components -- These 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 United States Coast Guard when operating as a Service in the Navy.

Federal Intelligence and Intelligence, Surveillance, and Reconnaissance Equipment -- Equipment purchased with Military Intelligence Program or National Intelligence Program monies.

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 c, including activities conducted by non-intelligence organizations.

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

Intelligence-Related Activity -- An activity outside the consolidated Defense intelligence program that responds to operational commanders' tasking for time-sensitive information on foreign entities; responds to national Intelligence Community tasking of systems with the primary mission of supporting operating forces; trains personnel for intelligence duties; provides an intelligence reserve; or is devoted to research and development of intelligence or related capabilities. Specifically excluded are programs so closely integrated with a weapon system that their primary function is to provide immediate-use targeting data.

Intelligence, Surveillance, and Reconnaissance -- An integrated operations and intelligence activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations.

National Guard Intelligence Component -- National Guard Bureau, Title 32, National Guard Joint Force Headquarters–State; 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 a Presidential directive, including references a, b, and c, this instruction, or other National Guard Bureau, Army, or Air Force policy documents and instructions.

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

Significant or Highly Sensitive Matter -- An intelligence or intelligence-related activity (regardless of whether it is unlawful or contrary to an Executive Order, Presidential directive, Intelligence Community Directive, or Department of Defense policy) or serious criminal activity by intelligence personnel that could impugn the reputation or integrity of the Intelligence Community, or otherwise call into question the propriety of intelligence activities. Such matters might involve actual or potential Congressional inquiries or investigations, adverse

media coverage, impact on foreign relations or foreign partners, or systemic compromise, loss, or unauthorized disclosure of protected information.

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; or 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.